TEMAS ATUAIS DE PROTEÇÃO DE DADOS PESSOAIS

REGINA LINDEN RUARO
GABRIELLE BEZERRA SALES SARLET
HELEN LENTZ RIBEIRO BERNASIUK
FERNANDA LINDEN RUARO PERINGER
ORGS.

Os textos selecionados gravitam em torno do eixo temático e caracterizam-se pela atualidade e relevância, de acordo com a acelerada dinâmica que marca a Sociedade da Informação, denominada também de Sociedade Digital. Cada artigo é uma peça valiosa do quebra-cabeça da proteção de dados pessoais, oferecendo perspectivas e insights que ajudarão a compreender as complexidades desse tema em constante evolução. A proteção de dados pessoais é um direito fundamental expresso no texto constitucional que, quando respeitado, pode contribuir para uma sociedade mais justa, ética e segura. Desejamos que o livro contribua para a construção de um futuro digital mais consciente e responsável. Agradecemos o apoio do PPGD da PUCRS, da Editora Fênix, das agências de fomento e que incentivam a pesquisa no nosso país, bem como aos autores dos textos que compõem essa obra.

As organizadoras.

9 786554 600712

Temas atuais de proteção de dados pessoais

Direção editorial: Ingo Wolfgang Sarlet
Diagramação: Editora Fundação Fênix
Concepção da Capa: Editora Fundação Fênix

O padrão ortográfico, o sistema de citações, as referências bibliográficas, o conteúdo e a revisão de cada capítulo são de inteira responsabilidade de seu respectivo autor.

A presente obra foi editada com apoio da Fundação de Amparo à Pesquisa do Estado do Rio Grande do Sul (FAPERGS), designadamente pelo Edital 09/2021 – AOE.

Série Direito – 85

Catalogação na Fonte

T278 Temas atuais de proteção de dados pessoais [recurso eletrônico] / Regina Linden Ruaro ... [et al.] Organizadoras. – Porto Alegre : Editora Fundação Fênix, 2023.
310 p. (Série Direito ; 85)

Demais organizadoras: Fernanda Linden Ruaro Peringer, Helen Lentz Ribeiro Bernasiuk, Gabrielle Bezerra Sales Sarlet.
Disponível em: <http://www.fundarfenix.com.br>
ISBN 978-65-5460-071-2
DOI https://doi.org/10.36592/9786554600712

1. Direito. 2. Inteligência artificial. 3. Proteção de dados. 4. Liberdade de expressão. 5. Brasil. Lei geral de proteção de dados pessoais (2018). I. Ruaro, Regina Linden (org.).

CDD: 340

Responsável pela catalogação: Lidiane Corrêa Souza Morschel CRB10/1721

SUMÁRIO

APRESENTAÇÃO 11

As Organizadoras

1. A NATUREZA JURÍDICA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): CONSIDERAÇÕES CONCEITUAIS E LEGAIS 13

Artur Hauser Schmitz

2. LEI 13.709/18 E O PAPEL DO CONSENTIMENTO – (ART. 7º) 31

Bernardo Spencer da Fontoura Teixeira

Laura Araujo Ribeiro Lino

3.* LIBERDADE DE EXPRESSÃO E MODERAÇÃO DE CONTEÚDO EM REDES SOCIAIS: *SHADOW BANNING 51

Fabrizio Predebon da Silva

***4.* INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE CIVIL: UMA ANÁLISE DOS MECANISMOS DE RESPONSABILIZAÇÃO NO BRASIL.** 75

Helen Lentz Ribeiro Bernasiuk

***5.* COLETA DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO: OS DESAFIOS DA DICOTOMIA NECESSIDADE X EXCESSO** 105

Regina Linden Ruaro

Jacqueline Varella

***6.* OBSTÁCULOS À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO** 133

Kim William Pinto Mendonça

7. DADOS PESSOAIS SENSÍVEIS: PROBLEMÁTICAS APLICADAS 153

Pedro Guilherme Müller Kurban

8. ASSÉDIO ELEITORAL NO AMBIENTE DE TRABALHO SOB A PERSPECTIVA DA LGPD: ANÁLISE JURISPRUDENCIAL APÓS ELEIÇÕES PRESIDENCIAIS NO BRASIL DE 2022 185
Plinio Gevezier Podolan

9. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO - ANÁLISE DO CAPÍTULO IV, DA LGPD, SEGUNDO AS DIRETRIZES EMITIDAS PELA ANPD EM SEU GUIA ORIENTATIVO DE 2022 211
Rafael Louzada Nardin

10. INTERNET DAS COISAS, CIDADES INTELIGENTES E O DIREITO À PRIVACIDADE DO CIDADÃO 229
Taina Daniele Werle

11. A LEI GERAL DE PROTEÇÃO DE DADOS EM CONSULTÓRIOS MÉDICOS 255
Taiane Meirelles Alfonsin

12. RESPONSABILIDADE CIVIL E O TRATAMENTO DE DADOS PESSOAIS NAS CIRURGIAS ROBÓTICAS 271
Victória Maltchik Salles Jung

13. PROTEÇÃO DE DADOS PELAS SERVENTIAS EXTRAJUDICIAS: UMA ANÁLISE A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E DO PROVIMENTO 134/CNJ 289
William Arthur Leonhardt Born

APRESENTAÇÃO

A proteção de dados pessoais nunca foi tão crucial quanto agora, porquanto vivemos em uma sociedade cada vez mais digital e interconectada. À medida que navegamos pelo mundo digital, compartilhamos informações sobre nossa vida, preferências e até mesmo nossa saúde em troca de serviços e conveniências. O risco da exposição indevida, abuso de dados e ameaças à privacidade é uma realidade que todos enfrentamos. Portanto, compreender as implicações legais e éticas é fundamental para construir um ambiente digital mais seguro e responsável. A presente obra é fruto de pesquisas de integrantes do Grupo de Pesquisas em Proteção de Dados Pessoais no Estado Democrático de da Pontifícia Universidade Católica do Rio Grande do Sul/PUCRS, integrado por textos de Docentes e Discentes, vinculados ao Programa de Pós-graduação em Direito (PUCRS). Composto por 13 artigos especializados que exploram diversos aspectos relacionados a esse tema premente. Alguns dos tópicos que serão discutidos incluem:

A Natureza Jurídica da Autoridade Nacional de Proteção de Dados (ANPD). Lei 13.709/18 e o Papel do Consentimento; a Liberdade de Expressão e Moderação de Conteúdo em Redes Sociais; a Inteligência Artificial e Responsabilidade Civil; a Coleta de Dados Pessoais nas Relações de Trabalho; os Obstáculos à Privacidade na Sociedade da Informação.

Dados Pessoais Sensíveis, o Assédio Eleitoral no Ambiente de Trabalho sob a Perspectiva da LGPD; o Tratamento de Dados Pessoais pelo Poder Público; a Internet das Coisas, Cidades Inteligentes e o Direito à Privacidade do Cidadão; A Lei Geral de Proteção de Dados em Consultórios Médicos; a Responsabilidade Civil e o Tratamento de Dados Pessoais nas Cirurgias Robóticas e, por fim, a Proteção de Dados pelas Serventias Extrajudiciais.

Os textos selecionados gravitam em torno do eixo temático e caracterizam-se pela atualidade e relevância, de acordo com a acelerada dinâmica que marca a Sociedade da Informação, denominada também de Sociedade Digital. Cada artigo é uma peça valiosa do quebra-cabeça da proteção de dados pessoais, oferecendo perspectivas e insights que ajudarão a compreender as complexidades desse tema em constante evolução.

A proteção de dados pessoais é um direito fundamental expresso no texto constitucional que, quando respeitado, pode contribuir para uma sociedade mais justa, ética e segura. Desejamos que o livro contribua para a construção de um futuro digital mais consciente e responsável.

Agradecemos o apoio do PPGD da PUCRS, da Editora Fênix, das agências de fomento e que incentivam a pesquisa no nosso país, bem como aos autores dos textos que compõem essa obra.

As organizadoras.

1. A NATUREZA JURÍDICA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): CONSIDERAÇÕES CONCEITUAIS E LEGAIS

https://doi.org/10.36592/9786554600712-01

Artur Hauser Schmitz[1]

RESUMO

Os avanços tecnológicos tornaram-se cotidianos nas últimas décadas, abrangendo uma série de áreas, como os dados pessoais e a privacidade dos cidadãos. Desta forma, impõe-se à sociedade e ao Estado construção de mecanismos capazes de proteger e preservar o direito fundamental à proteção de dados pessoais, conforme disposto no Art. 5º, Inciso LXXIX da Carta Magna. Neste panorama, situa-se a Autoridade Nacional de Proteção de Dados (ANPD), cuja principal função é resguardar a proteção de dados pessoais e por regulamentar, efetivar e supervisionar o cumprimento da LGPD no país. A Lei nº 14.460/2022 concebeu à ANPD a natureza jurídica de Autarquia em Regime Especial, com *status* de agência reguladora. Verifica-se, portanto, construção jurídico-administrativa da ANPD desta forma é crucial para que ela possua autonomia orçamentária, operacional e reguladora para exercer com eficácia as suas funções indispensáveis, cuja principal é a proteção de um direito fundamental.
Palavras-chave: Proteção de Dados; Autoridade Nacional de Proteção de Dados; Natureza Jurídica.

ABSTRACT

Technological advances have become everyday in recent decades, covering a number of areas, such as personal data and privacy of citizens. In this way, society and the State are required to build mechanisms capable of protecting and preserving the fundamental right to the protection of personal data, as provided for in Article 5, Item LXXIX of the Magna Carta. In this scenario, the National Data Protection Authority (ANPD) is located, whose main function is to safeguard the protection of personal data and to regulate, enforce and supervise compliance with the LGPD in the country. Law No. 14,460/2022 gave the ANPD the legal nature of an Autarchy under a Special Regime, with the status of a regulatory agency. Therefore, the legal-administrative construction of the ANPD is therefore crucial for it to have budgetary, operational and regulatory autonomy to effectively exercise its indispensable functions, the main of which is the protection of a fundamental right.
Keywords: Data Protection; National Data Protection Authority; Legal Nature.

[1] Graduando em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) e em Administração pela Universidade Federal do Rio Grande do Sul (UFRGS). Participante do programa G+1 (Integração da Graduação e do Mestrado) da Escola de Direito da PUCRS. E-mail: arturhauserschmitz@gmail.com e artur.schmitz@edu.pucrs.br

1 Introdução

Os avanços tecnológicos vistos na última década demonstraram-se dignos de preocupação dos mais diversos setores da sociedade. A participação ativa das tecnologias no cotidiano do cidadão (no uso contínuo das redes sociais, por exemplo) determinou uma resposta estatal efetiva, visando assegurar o respeito adequado aos "usuários" do mundo digital, abrangendo as mais diversas áreas de estudos.

O Direito Fundamental à Proteção de Dados Pessoais é basilar no âmbito de uma sociedade movida à informação digital, na qual os dados pessoais são motivo, inclusive, de comercialização intensa[2]. Tanto que o Art. 5o, Inciso LXXIX da Carta Magna, incluído pela Emenda Constitucional (EC) No 115/2022, determina que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais".

Com a aprovação da Lei Geral de Proteção de Dados (LGPD), Lei n. 13.709 de 14 deagosto de 2018, anterior a EC 115/2022, fora gerado um impasse acerca da criação (ou não)de um órgão estatal cuja principal função fosse fiscalizar, regular e se fazer cumprir a LGPD[3]. Um consenso nítido, apesar das pressões externas fomentadas por empresas do ramo: a não implementação deste organismo prejudicaria frontalmente a efetivação da proteção deste Direito Fundamental.

Sendo assim, a criação de uma Autoridade Nacional de Proteção de Dados foi assentada pela doutrina referência no tema e pelo Parlamento Brasileiro. Tal panorama demandou uma série de mecanismos que possibilitasse a sua atuação concreta, conforme se verá a seguir.

---

[2] MARTÍNEZ, Gabriel Francisco Cevallos; DAMASCENO, Handherson Leyltton Costa; MACEDO, Társio Roberto Lopes. Privacidade e redes digitais: a comercialização de dados no ciberespaço. **Revista e-Curriculum**,v. 17, n. 3, p. 1393-1398, 2019.

[3] LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados.** Lisboa (Portugal): Grupo Almedina (Portugal), 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 11 jun. 2023.

2 A Proteção de Dados Pessoais como um Direito Fundamental

Primeiramente, cabe destacar que a proteção de dados sociais atingiu, merecidamente, a posição de (i) Direito Fundamental; e (ii) possuindo expressa positivação na Carta Magna. Em relação ao primeiro ponto, compreende-se que um Direito Fundamental é, segundo a doutrina especializada, aqueles "concebidos como aqueles direitos (dentre os quais se destacam os direitos humanos) reconhecidos e positivados na esfera do direito constitucional"[4].

Possível aferir, também, que se trata de direito positivamente expresso, uma vez que possui previsão nominal no Art. 5o, Inciso LXXIX, da Carta Magna, conforme respaldado pela doutrina:

> [...] a) direitos expressamente positivados, seja na Constituição, seja em outros diplomas jurídico-normativos de natureza constitucional; (b) direitos implicitamente positivados, no sentido de direitos fundamentais decorrentes do regime e dos princípios constitucionais ou direitos subentendidos nas normas de direitos fundamentais expressamente positivadas, em suma, direitos que não encontram respaldo textual direto, podendo também ser designados de direitos não escritos."[5]

A revolução informacional apresenta estreita ligação com os avanços tecnológicos e comunicacionais[6], cujas consequências no âmbito de dados são de extrema relevância. Imperioso considerar que a preocupação protetora para com este direito fundamental já vinha em processo de solidificação legal e doutrinária, não obstante o significativo avanço tecnológico percebido nas últimas décadas.

Observa-se, nesta conjuntura, o surgimento de uma compreensão acerca do vínculo entre o direito fundamental à proteção de dados e outros da mesma estatura:

---

[4] SARLET, Ingo W.; MARINONI, Luiz G.; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Editora Saraiva, 2022. *E-book.* ISBN 9786553620490. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620490/. Acesso em: 10 mai. 2023.

[5] SARLET, MARINONI, MITIDIERO, op. cit.,

[6] ROZA, R. H. Revolução Informacional e os Avanços Tecnológicos da Informática e das Telecomunicações. **Ciência da Informação em Revista**, *[S. l.]*, v. 4, n. 3, p. 3–11, 2017. DOI: 10.28998/cirev.2017v4n3a. Disponível em: https://www.seer.ufal.br/index.php/cir/article/view/3482. Acesso em: 26 ago. 2023.

> Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana [...][7]

A comunidade europeia, em especial a germânica, já vinha realizando contundentes estudos acerca do tema, enfatizando a premência de se construir mecanismos protetores dos dados pessoais. Esta conjuntura culminou em elevar, pela primeira vez, como um direito de cunho fundamental:

> E foi da experiência europeia, mais especificamente, do protagonismo alemão nessa área que remonta aos anos setenta do século passado, que adveio o legado quanto à proteção de dados nos moldes atuais e, nesse sentido, o seu reconhecimento como umdireito humano e fundamental. (...) Com efeito, a LGPD dispõe, em seu artigo 1o , sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[8]

Outra fonte de preocupação latente é o uso inadequado de dados pessoais, inlcusive na sua potencial comercialização. Apesar deste fenômeno ter ganhado mais destaque nos últimos tempos, observa-se que ja No comunidade europeia, alertava-se, há tempos, que a comunidade jurídica internacional já alertava para esta problemática:

---

[7] WOLFGANG SARLET, I.; AGOSTINI SAAVEDRA, G. FUNDAMENTOS JUSFILOSÓFICOS E ÂMBITO DE PROTEÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. **Direito Público**, [S. l.], v. 17, n. 93, 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 29 ago. 2023.

[8] SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021.

> Es evidente que, en nuestros días, una de las amenazas potencialmente más intensas y determinantes contra la intimidad, el honor y, en geral, los derechos de las personas , puede provenir de la manipulación o incluso del uso inadecuado de datos que le conciernan y que pueden estar incorpados a diferentes soportes físicos, especialmente a aquellos que sean susceptibles a tratamiento informático. Tal possibilidad es debida a la extraordinaria diversficiación de los intereses públicos y privados generada en torno al conocimiento, manejo y, en su caso, comercialización de determinados datos de caráter personal , junto con los cada vez más intensos y acelerados avances tecnológicos en este terreno, que permite amplias y muy variadas formas de cruce y asociació de tales datos conducentes a la elaborácion de 'perfiles' de personalidad.[9]

A partir da necessidade de devida proteção deste Direito Fundamental, cristalizou-se a imprescindibilidade de se criar e de se consolidar este órgão protetor. Ou seja, a presença de uma entidade independente - financeira e administrativamente - é indispensável para a ampliação da tutela defensiva dos dados pessoais dos brasileiros.

3 O histórico legislativo da Autoridade Nacional de Proteção de Dados (ANPD)

A trajetória legislativa da criação e da estruturação da ANPD deve ser dividida em quatro fases: (i) criação; (ii) transformação em autarquia de natureza especial; (iii) vinculação ao Ministério da Justiça e Segurança Pública; e (IV) estruturação regimental e operacional.

Em relação ao primeiro ponto, observa-se que a criação da ANPD fora possível por meio da edição da Medida Provisória (MP) nº 869, de 2018, convertida na Lei nº 13.853, de 08 de julho de 2019, que alterou a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709, de 14 de agosto de 2018): "Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a

---

[9] CALLEJÓN, Francisco Balaguer; VILLAR, Gregório Cámara; AGUILAR, Juan Fernando López, CALLEJÓN, Maria Luisa Balaguer; MARTOS, José Antonio Montilla. **Manual de Derecho Constitucional**, Vol. II, Quinta Edição, Editora Tecnos, Madri (Espanha), 2010.

Autoridade Nacional de Proteção de Dados; e dá outras providências"[10].

Ademais, atesta-se que esta mesma lei previu a composição da Diretoria da ANPD, doConselho Nacional de Proteção de Dados Pessoais e da Privacidade, da Corregedoria da ANPD, bem como de sua Ouvidoria, todas estas alterações sem aumento de despesa à época.

A ANPD passou, portanto, a funcionar efetivamente com a nomeação de seu primeiro Diretor-Presidente, Waldemar Gonçalves Ortunho Júnior, datada de 05 de novembro de 2020,presente no Diário Oficial da União:

> O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84,caput, inciso XIV, da Constituição, e tendo em vista o disposto no art. 55-D da Lei nº 13.709, de 14 de agosto de 2018, resolve: NOMEAR WALDEMAR GONÇALVES ORTUNHO JUNIOR, para exercer o cargo de Diretor-Presidente do Conselho Diretor da Autoridade Nacional de Proteção de Dados - ANPD, com mandato de seis anos[9].

Ademais, as estruturas gerencial e operacional da ANPD passaram também foram delimitadas, sendo que seus respectivos gestores também passaram a exercer as suas funções. Vale a transcrição de trecho da Lei nº 13.853:

> Art. 55-C. A ANPD é composta de: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; Conselho Diretor da ANPD será composto de 5 (cinco) diretores, incluído o Diretor-Presidente. § 1º Os membros do Conselho Diretor da ANPD serão escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal, nos termos da alínea 'f' do inciso III do art. 52 da Constituição Federal, e ocuparão cargo emcomissão do Grupo-Direção e Assessoramento Superiores - DAS, no mínimo, de nível 5. § 2º Os membros do Conselho Diretor serão escolhidos dentre brasileirosque tenham reputação ilibada, nível superior de educação e elevado conceito no campo de

[10] BRASIL. Congresso Nacional. **Lei nº 13.853, de 8 de julho de 2019.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 02 mai. 2023.

> especialidade dos cargos para os quais serão nomeados. § 3º O mandato dos membros do Conselho Diretor será de 4 (quatro) anos. § 4º Os mandatos dos primeiros membros do Conselho Diretor nomeados serão de 2 (dois), de 3 (três), de 4 (quatro), de 5 (cinco) e de 6 (seis) anos, conforme estabelecido no ato de nomeação. § 5º Na hipótese de vacância do cargo no cu do mandato de membro do Conselho Diretor, o prazo remanescente será completado pelo sucessor.

Portanto, compreende-se que a ANPD apresenta: I - Conselho Diretor, órgão máximo de direção; II - Conselho Nacional de Proteção de Dados Pessoais e da Privacidade; III - Corregedoria; IV - Ouvidoria; V - órgão de assessoramento jurídico próprio; e VI - unidades administrativas e unidades especializadas necessárias à aplicação do disposto nesta Lei. Um ponto importante é relacionado à subordinação da ANPD à Presidência da República, conforme ditava o Art. 55-A:

> Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, **submetida a regime autárquico especial e vinculada à Presidência da República.** 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.[11]

Tal previsão fora amplamente criticada pela doutrina especializada, uma vez que mantinha a subalternidade da ANPD ao Presidente da República, prejudicando a sua independência administrativa e financeira[12], inclusive na própria nomeação dos

[11] **BRASIL, Congresso Nacional.** op. cit.
[12] COPETTI, Rafael; CELLA, José Renato Gaziero. A salvaguarda da privacidade e a autoridade nacional de proteção de dados. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 1, p. 44-62, 2019.

membros do Conselho Nacional de Proteção de Dados Pessoais (CNPDP)[13].

Nesta perspectiva, pesquisadores da área já sinalizavam a importância da presença de um órgão com autonomia plena (administrativa, orçamentária e financeira):

> Ainda, o referido projeto de lei dispõe sobre a criação do Conselho Nacional de Proteção de Dados Pessoais (art. 38) que contará com autonomia administrativa, orçamentária e financeira com a competência de atuar como Autoridade de Garantia na matéria, remetendo a uma legislação específica a sua estruturação e o conjunto de atribuições. Possivelmente o Conselho se constituirá sob a forma de autarquia já que é bem provável que o mesmo tenha atue como agência reguladora.[14]

Imprescindível considerar que a falta de autonomia funcional é motivo de preocupação, uma vez que põe em dúvida a efetiva operacionalização da razão de ser da ANPD: proteger os dados pessoais dos cidadãos brasileiros.

Este panorama é solucionado pela edição da Medida Provisória nº 1.124, de 13 dejunho de 2022, convertida na Lei nº 14.460, de 25 de outubro de 2022, alterando a Lei nº 13.709/2018, concebendo à Autoridade Nacional de Proteção de Dados o regime jurídico de autarquia de natureza especial, tema do segundo ponto apresentado.

Constata-se crucial a referência aos dispositivos que culminaram nesta importante mudança:

> Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados; altera as Leis nºs 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais), e 13.844, de 18 de junho de 2019; e revoga dispositivos da Lei nº 13.853, de 8 de

---

[13] **DONEDA, Danilo.** Da privacidade à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2021, p. 333

[14] RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A PRIVACIDADE. **Revista da Faculdade de Direito UFPR**, Curitiba, v. 53, jun. 2011. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 29 ago. 2023. doi:http://dx.doi.org/10.5380/rfdufpr.v53i0.30768.

> julho de 2019. Faço saber que o PRESIDENTE DA REPÚBLICA adotou a Medida Provisória nº 1.124, de 2022, que o Congresso Nacional aprovou, e eu, Rodrigo Pacheco, Presidente da Mesa do Congresso Nacional, para os efeitos do disposto no art. 62 da Constituição Federal, com a redação dada pela Emenda Constitucional nº 32, combinado com o art. 12 da Resolução nº 1, de 2002-CN, promulgo a seguinte Lei **Art. 1º Fica a Autoridade Nacional de Proteção de Dados (ANPD) transformada em autarquia de natureza especial, mantidas a estrutura organizacional e as competências e observados os demais dispositivos da Lei nº 13.709, de 14 de agosto de 2018.**[15]

A partir do exposto, considera-se que a alçada da ANPD ao patamar de autarquia de natureza especial é fato importante para a devida efetivação de suas funções primordiais para a efetiva proteção de dados.

Em relação à vinculação da ANPD ao Ministério da Justiça e Segurança Pública(MJSP), revela-se fundamental destacar o Decreto N. 11.401/2023, o qual reformulou as vinculações das entidades da Administração Pública Indireta:

> **O VICE-PRESIDENTE DA REPÚBLICA**, no exercício do cargo de Presidente da República, no uso da atribuição que lhe confere o art. 84, **caput**, inciso VI, alínea "a", da Constituição, DECRETA: (...) Artigo único. A vinculação das entidades da administração pública federal indireta é a seguinte: (...) XV - ao Ministério da Justiça e Segurança Pública: a) Conselho Administrativo de Defesa Econômica - Cade; e b) Autoridade Nacional de Proteção de Dados - ANPD;[16]

Observa-se, por fim, que as estrutura regimental e operacional da Autoridade foram dispostas Decreto nº 10.474, de 26 de agosto de 2020, alterada pelo Decreto nº 10.975, de 22 de fevereiro de 2022, e, posteriormente, pelo Decreto nº 11.202, de 21 de setembro de 2022, sendo que este último confere nova redação ao Art. 1º do Decreto nº 10.474, de 26 de agosto de 2020:

---

[15] BRASIL. Congresso Nacional. Lei nº 14.460, de 25 de outubro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 02 mai. 2023.

[16] BRASIL. Decreto nº 11.401, de 23 de janeiro de 2023. PRESIDÊNCIA DA REPÚBLICA. ALCKMIN FILHO, GERALDO JOSÉ RODRIGUES et al Disponível em: https://dspace.mj.gov.br/bitstream/1/8816/1/DEC_PR_2023_11401.pdf > . Acesso em: 02 mai. 2023.

> Art. 1º A Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial vinculada à Casa Civil da Presidência da República, dotada de autonomia técnica e decisória, com patrimônio próprio, jurisdição no território nacional e sede e foro em Brasília, Distrito Federal, tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, orientada pelo disposto na Lei nº 13.709, de 14 de agosto de 2018.[17]

Relevante considerar, portanto, que a cronologia legislativa e infralegal da ANPDrepresenta um marco importante em relação à consolidação desta instituição no âmbito da proteção de dados pessoais dos brasileiros, principalmente na sua elevação ao *status* deAutarquia em Regime Especial.

4 Regime Jurídico da ANPD

Primeiramente, salienta-se que as autarquias estão previstas no Art. 37. Inciso XIX da Carta Magna, o qual preceitua:

> [...]somente por lei específica poderá ser criada autarquia e autorizada a instituição de empresa pública, de sociedade de economia mista e de fundação, cabendo à lei complementar, neste último caso, definir as áreas de sua atuação;[18]

A Lei nº 14.460, de 25 de outubro de 2022 concebeu, conforme citado anteriormente, a ANPD como uma autarquia em regime especial, sendo, mais especificamente, uma agência reguladora. A devida conceituação de "autarquia de natureza especial" recebe tratamento exemplar na doutrina:

> Já antecipamos que a natureza jurídica das agências reguladoras é a de autarquias, sendo, portanto, dotadas de personalidade jurídica de direito público.

[17] BRASIL. Decreto nº 11.202, de 23 de janeiro de 2023. PRESIDÊNCIA DA REPÚBLICA. JAIR MESSIAS BOLSONARO et al. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20192022/2022/decreto/D11202.htm#:~:text=Altera%20o%20Decreto%20n%C2%BA%2010.474,9.660%2C%20de%201%C2%BA%20de%20janeiro>

[18] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil. Brasília**, DF: Senado Federal, 2016. 496 p. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 24 maio 2023.

> Trata-se de entes públicos da administração indireta do Estado, com a função específica de controle de atividades econômicas e da prestação de serviços públicos. Dentro do gênero autarquias, as agências reguladoras situam-se na categoria das autarquias especiais, ou, se assim se preferir, autarquias de regime especial, **pela circunstância, já anotada, de que seu regime jurídico se apresenta com certas peculiaridades específicas, não incidentes sobre as autarquias comuns, ou de regime comum**.[19]

Marçal Jutsten Filho enfatizada o caráter autônomo destas autarquias, fator determinante para que elas exercem corretamente as suas funções constitucionais :

> Uma agência reguladora independente consiste em uma autarquia especial, o que significa que a Lei instituidora prevê algumas peculiaridades no regime jurídico aplicável à entidade, **propiciando uma margem de autonomia jurídica que não se encontra na maior parte das entidades autárquicas. Isso envolve a redução do grau de subordinação da entidade em face da Administração direta.** Há um regime especial de investidura e demissão dos administradores das agências, os quais são providos em cargos em comissão por prazo certo e sujeitos à demissão apenas em virtude da prática de atos irregulares (tal como adiante será mais bem examinado).[20]

Esta caracterização culmina em uma série de aspectos práticos à Autoridade, tanto do ponto de vista funcional quanto do ponto orçamentário, típicos de agência reguladoras. Essencial, portanto, compreender que as forças institucional e funcional das agências reguladoras se intensificaram de forma considerável, principalmente nas últimas décadas.

A função "normativa" das agências reguladoras, destaca-se, não se sobrepõe aos regramentos dispostos pelo legislador, pelo contrário, submetem-se aos preceitos legais e constitucionais vigentes. A edição de atos normativos

---

[19] FILHO, José dos Santos C. **Manual de Direito Administrativo**. São Paulo: Grupo GEN, 2022. *E-book*. ISBN9786559771837. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771837/. Acesso em:12 jun. 2023.

[20] FILHO, Marçal J. **Curso de Direito Administrativo**. São Paulo: Grupo GEN, 2023. *E-book*. ISBN 9786559645770. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559645770/. Acesso em:12 jun. 2023.

infralegais, também denominado de “deslegalização”, é consoante ao ordenamento jurídico pátrio:

> Nessa ordem de convicções, é jurídico sustentar a constitucionalidade do exercício da função normativa “secundária” pelas entidades reguladoras por não se detectar, pela via da deslegalização, qualquer usurpação da função legiferante, de competência do Poder Legislativo, nem, tampouco, do poder regulamentar de atribuição precípua do chefe do Poder Executivo.[21]

Tal cenário possibilita, inclusive, que a capacidade técnica das agências seja amplamente reconhecida, possibilitando a adequada imposição de obrigações aos seus regulados[22].

Na perspectiva comparada, mais especificamente no cenário norte-americano, o já denominado “poder normativo” é delegado pelo Legislativo, fato que simboliza a independência das agências reguladoras:

> 2. A independência das agências administrativas reguladoras se manifesta principalmente através do exercício de poder normativo; 3. A função normativa das agências administrativas consiste em poder delegado pelo Legislativo para editar regulamentos;[23]

Nesta seara, a devida estruturação de uma autarquia do tipo deve apresentar meios de operacionalizar a sua atuação, conforme explicita a doutrina especializada:

> a) Agências Reguladoras: são espécies de autarquias em regime especial e possuem como finalidade principal regulamentar e fiscalizar a prestação dos serviços públicos realizada por particulares. São exemplos de agências

---

[21] GUERRA, Sérgio. Função normativa das agências reguladoras: uma nova categoria de direito administrativo?. **Revista direito GV**, v. 7, p. 131-152, 2011.

[22] MAFFINI, Rafael Da Cás; MARÇAL, Thaís Boia. ESG e o projeto da nova lei de licitações e contratos administrativos. **Revista Digital da ESA-OABRJ. Rio de Janeiro: ESA-OABRJ. Vol. 3, ano 3 (2021), p. 1111-1114.**, 2021.

[23] CUÉLLAR, L. Poder normativo das agências reguladoras norte-americanas. **Revista de Direito Administrativo**, *[S. l.]*, v. 229, p. 153–176, 2002. DOI: 10.12660/rda.v229.2002.46435. Disponível em: https://periodicos.fgv.br/rda/article/view/46435. Acesso em: 29 ago. 2023.

> reguladoras a ANATEL (Agência Nacional de Telecomunicações), que regulamenta a prestação do serviço de telecomunicações pelos particulares, e a ANEEL (Agência Nacional de Energia Elétrica), que regulamenta a prestação do serviço de transmissão e distribuição de energia elétrica feita por particulares. Caracterizam o aludido regime especial (regras específicas das agências reguladoras, que as diferenciam das demais autarquias): **(i) o mandatofixo dos seus dirigentes (só perderão o cargo por processo administrativo ou judicial ou por renúncia); (ii) a imutabilidade de suas decisões (não podem ser alteradas pela Administração Direta); (iii) o período de quarentena (tempo em que o ex-dirigente da agência reguladora ficará fora do mercado de trabalho no setor da regulação)50; e (iv) poder normativo ou regulatório (poder das agências de expedir normas técnicas do setor de regulação, como as resoluções, que são atos administrativos infralegais)**.[24]

Salienta-se que, no âmbito jurídico-administrativo pátrio, as agências reguladoras exercem suas atividades (regulatória e sancionatória, por exemplo) vinculadas atividades específicas, como a aviação civil (sob fiscalização da Agência Nacional de Aviação Civil) e o setor de mineração (exercido pela Agência Nacional de Mineração):

> Atentemos para o fato de que cada uma dessas agências está relacionada a um determinado setor da atividade econômica, cuja fiscalização pelo Poder Público justifica-se pela necessidade do atendimento do interesse público, identificado como o interesse dos administrados, destinatários e usuários dos serviços públicos ou serviços de interesse público objetos da regulação.[25]

Danilo Doneda já defendia que a "(...) das configurações para este órgão, identificamos opções como a de um órgão funcionalmente independente da estrutura estatal, de perfil que genericamente associamos no Brasil a uma agência

---

[24] ALMEIDA, Fabrício Bolzan de. **Manual de direito administrativo**. São Paulo: Editora Saraiva, 2022.*E-book.*Disponívelem: https://integrada.minhabiblioteca.com.br/#/books/9786553620421/. Acesso em: 12 jun. 2023.

[25] ROSA, R. P. de A. Reflexões sobre a função reguladora das agências estatais. **Revista de Direito Administrativo**, *[S. l.]*, v. 226, p. 243–250, 2001. DOI: 10.12660/rda.v226.2001.47244. Disponível em: https://periodicos.fgv.br/rda/article/view/47244. Acesso em: 28 ago. 2023.

(...)"[26].

Observa-se, a partir deste panorama, que a ANPD carrega consigo responsabilidades de cunho constitucional, protegendo e efetivando os direitos assegurados na Carta Magna.

Diferentemente de outras autarquias em regime especial, a ANPD protege e preserva um direito fundamental, não tendo sob a sua vigilância um setor específico em si, mas toda e qualquer atividade que lide com dados pessoais, ou seja, quase a sua totalidade.

Ou seja, atesta-se que as garantias funcionais concedidas pelo legislador à ANPD fazem jus a sua relevância, ainda mais com o constante avanço dos meios tecnológicos. Neste horizonte, sublinha-se a pertinência sociológica das agências reguladoras:

> Sob o ponto de vista sociológico, o papel das agências reguladoras vem sendo redefinido com o fito de realizar interesses comuns da sociedade, e não apenas o caráter econômico dos agentes de mercado. Acresce-se aos sujeitos da relação, além do Estado e dos agentes econômicos, o cidadão — destinatário final da atividade regulatória dos serviços públicos. A partir destes novos parâmetros, um novo modelo de conduta e uma nova relação social foram criados, gerando uma evolução no conceito e no papel do instituto jurídico das agências reguladoras.[27]

Em vista disso, compreende-se que o modelo vinculado à ANPD é o mais adequado, considerando-se (i) a maior independência funcional e técnica de seus funcionários; (ii) o poder normativo e regulatório; e (iii) a imutabilidade das suas decisões perante a Administração Direta.

Esta indispensabilidade é consequência da atuação das agências reguladoras para minimizar os danosos efeitos da concentração de poder, seja pela via econômica, seja pela via política:

---

[26] DONEDA, op. cit., p. 335

[27] DE CARVALHO, Ivo César Barreto. O papel das agências reguladoras como propulsoras de mudança social. **Revista da Faculdade de Direito**, v. 34, n. 2, p. 173-196, 2013.

> A instituição da agência independente reflete, então, a ampliação da complexidade do sistema de freios e contrapesos. Visam a atenuar a concentração de poder, ampliando o número de instituições estatais dotadas de competências decisórias e limitando o âmbito de atuação dos governantes eleitos (sejam eles integrantes do Executivo ou do Legislativo).[28]

Sendo assim, é evidente que a ANPD passe a exercer as suas atribuições consubstanciadas de estruturas técnica e humana, capazes de eficazmente permitirem uma fiscalização efetiva da LGPD e, consequentemente, a proteção de um direito fundamental dos brasileiros.

Conclusão

As ameaças de vazamento ou de tratamento inadequado de dados são frequentes no cenário contemporâneo, demandando, portanto, que haja um órgão capaz de fiscalizar estas atividades e resguardar este direito fundamental.

A partir do exposto, ressalta-se que a criação da ANPD surge na esteira da evidentenecessidade da presença de uma entidade independente - financeira e administrativamente - para tutelar defensivamente os dados pessoais dos brasileiros.

Os direitos fundamentais inerentes à proteção de dados (como a privacidade e a dignidade da pessoa humana), somados aos constantes avanços tecnológicos, apresentam suficiente condão para que a ANPD não restrinja a sua atuação a uma área em específico.

Tal panorama é o ideal para a consolidação dos mecanismos protetores do Direito Fundamental à Proteção de Dados Pessoais: um órgão estatal cuja principal função fosse fiscalizar, regular e se fazer cumprir a LGPD.

Compreende-se que a Lei nº 14.460, de 25 de outubro de 2022 concebeu, conformecitado anteriormente, a ANPD como uma autarquia em regime especial, sendo, mais especificamente, uma agência reguladora, conferindo-lhe (i) a maior

---

[28] JUSTEN FILHO, Marçal. Agências reguladoras e democracia: existe um déficit democrático na "regulação independente". **ARAGÃO, Alexandre Santos de. O poder normativo das agências reguladoras. Rio de Janeiro: Forense**, p. 301-332, 2006.

independência funcional e técnica de seus funcionários; (ii) poder normativo e regulatório; e (iii) imutabilidade das duas decisões perante a Administração Direta.

Portanto, compreende-se a existência de um cenário político-administrativo capaz de substanciar a devida atuação da ANPD, bastando que ela continue cumprindo as suas funções, cuja extrema relevância é indiscutível.

Referências

ALMEIDA, Fabrício Bolzan de. **Manual de direito administrativo**. São Paulo: Editora Saraiva, 2022. *E-book.* ISBN 9786553620421. Disponível em:https://integrada.minhabiblioteca.com.br/#/books/9786553620421/. Acesso em: 12jun. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil.** Brasília, DF: Senado Federal, 2016. 496 p. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 24 maio 2023.

BRASIL. Congresso Nacional. **Lei nº 13.853, de 8 de julho de 2019**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acessoem: 02 mai. 2023.

BRASIL. Congresso Nacional. **Lei nº 14.460, de 25 de outubro de 2022**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm.Acesso em: 02 mai. 2023.

BRASIL. **Decreto nº 11.401, de 23 de janeiro de 2023**. PRESIDÊNCIA DA REPÚBLICA. ALCKMIN FILHO, GERALDO JOSÉ RODRIGUES et al. Disponívelem < https://dspace.mj.gov.br/bitstream/1/8816/1/DEC_PR_2023_11401.pdf > ;

CALLEJÓN, Francisco Balaguer; VILLAR, Gregório Cámara; AGUILAR, Juan Fernando López, CALLEJÓN, Maria Luisa Balaguer; MARTOS, José Antonio Montilla. **Manual de Derecho Constitucional**, Vol. II, Quinta Edição, Editora Tecnos, Madri (Espanha), 2010.

COPETTI, Rafael; CELLA, José Renato Gaziero. A salvaguarda da privacidade e a autoridade nacional de proteção de dados. **Revista de Direito, Governança e Novas Tecnologias**, v. 5, n. 1, p. 44-62, 2019.

CUÉLLAR, L. Poder normativo das agências reguladoras norte-americanas. **Revista de Direito Administrativo**, *[S. l.]*, v. 229, p. 153–176, 2002. DOI: 10.12660/rda.v229.2002.46435. Disponível em: https://periodicos.fgv.br/rda/article/view/46435. Acesso em: 29 ago. 2023.

DE CARVALHO, Ivo César Barreto. O papel das agências reguladoras como propulsoras de mudança social. **Revista da Faculdade de Direito**, v. 34, n. 2, p. 173-196, 2013.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 2011.

________. Da privacidade à Proteção de Dados Pessoais. São Paulo: Revista dos Tribunais, 2021. **Espaço Jurídico Journal of Law [EJJL]**, v. 12, n. 2, p. 91-108, 2011.

FILHO, José dos Santos C. **Manual de Direito Administrativo**. São Paulo: Grupo GEN, 2022. *E-book.* ISBN 9786559771837. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559771837/. Acesso em: 12jun. 2023.

FILHO, Marçal J. **Curso de Direito Administrativo**. São Paulo: Grupo GEN, 2023. *E-book.* ISBN 9786559645770. Disponível em:https://integrada.minhabiblioteca.com.br/#/books/9786559645770/. Acesso em: 12jun. 2023.

GUERRA, Sérgio. Função normativa das agências reguladoras: uma nova categoria de direito administrativo?. **Revista direito GV**, v. 7, p. 131-152, 2011.

JUSTEN FILHO, Marçal. Agências reguladoras e democracia: existe um déficit democrático na "regulação independente". **ARAGÃO, Alexandre Santos de. O poder normativo das agências reguladoras. Rio de Janeiro: Forense**, p. 301-332, 2006.

LIMA, Cíntia Rosa Pereira de. **Autoridade nacional de proteção de dados e a efetividade da Lei Geral de Proteção de Dados. (Coleção teses de doutoramento)**. Lisboa: Grupo Almedina (Portugal), 2020. *E-book.* ISBN 9788584936397. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584936397/. Acesso em: 11 jun. 2023.

MARTÍNEZ, Gabriel Francisco Cevallos; DAMASCENO, Handherson Leyltton Costa; MACEDO, Társio Roberto Lopes. Privacidade e redes digitais: a comercialização de dados no ciberespaço. **Revista e-Curriculum**, v. 17, n. 3, p.1393-1398, 2019.

ROSA, R. P. de A. Reflexões sobre a função reguladora das agências estatais. **Revista de Direito Administrativo**, *[S. l.]*, v. 226, p. 243–250, 2001. DOI: 10.12660/rda.v226.2001.47244. Disponível em: https://periodicos.fgv.br/rda/article/view/47244. Acesso em: 28 ago. 2023.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize. O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A PRIVACIDADE. **Revista da Faculdade de Direito UFPR**, Curitiba, v. 53, jun. 2011. ISSN 2236-7284. Disponível em: <https://revistas.ufpr.br/direito/article/view/30768>. Acesso em: 29 ago. 2023. doi:http://dx.doi.org/10.5380/rfdufpr.v53i0.30768.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021.

SARLET, Ingo W.; MARINONI, Luiz G.; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Editora Saraiva, 2022. *E-book.* ISBN 9786553620490. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620490/. Acesso em: 10 mai. 2023.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. Lisboa (Portugal): GrupoAlmedina (Portugal), 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 11 jun. 2023.

SARLET, Ingo W.; MARINONI, Luiz G.; MITIDIERO, Daniel. **Curso de direito constitucional**. São Paulo: Editora Saraiva, 2022. *E-book.* ISBN 9786553620490. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553620490/. Acesso em: 10 mai. 2023.

WOLFGANG SARLET, I.; AGOSTINI SAAVEDRA, G. FUNDAMENTOS JUSFILOSÓFICOS E ÂMBITO DE PROTEÇÃO DO DIREITO FUNDAMENTAL À PROTEÇÃO DE DADOS PESSOAIS. **Direito Público**, [S. l.], v. 17, n. 93, 2020. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 29 ago. 2023.

2. LEI 13.709/18 E O PAPEL DO CONSENTIMENTO – (ART. 7º)

LAW 13.709/18 AND THE ROLE OF CONSENT – (ART. 7)

https://doi.org/10.36592/9786554600712-02

Bernardo Spencer da Fontoura Teixeira[1]

Laura Araujo Ribeiro Lino[2]

SUMÁRIO

Introdução; 1. A proteção de dados pessoais como direito fundamental autônomo; 2. LGPD e suas similaridades com o GDPR; 3. Consentimento do titular e as bases legais do art. 7º da LGPD; 4. A manifestação livre e o desbalanceamento do consentimento; 5. Desafios da base legal do consentimento no âmbito das crianças e dos adolescentes; Considerações Finais; Referências.

RESUMO

A crescente propagação dos dados pessoais, decorrente do acentuado desenvolvimento do setor da tecnologia, inserido em um ambiente pautado pela globalização, impulsionou o desenvolvimento de instrumentos jurídicos específicos aptos a tutelar os direitos decorrentes de situações relativas ao "mundo" digital. Diante desse cenário, a legislação brasileira de proteção de dados, a LGPD, conferiu especial relevância ao regulamento do consentimento, como uma das bases de tratamento de dados, de modo a demonstrar a sua preocupação com a participação do indivíduo no fluxo de suas informações. Portanto, com o presente trabalho, intui-se analisar a consentimento positivado no art. 7º da LGPD, bem como os seus aspectos históricos e as suas repercussões práticas.
Palavras-chaves: Proteção de dados pessoais. Lei Geral de Proteção de Dados (LGPD). Consentimento. Art. 7º.

ABSTRACT

The increasing propagation of personal data that is due to the rising development in the technology industry, inserted in an environment guided by globalization, has driven the development of specific legal instruments which are able to protect the rights due to situations relating to the "digital world". In light of this situation, the

[1] Mestrando em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS) - Bolsista CAPES Taxas. Bacharel em Direito pela Fundação Escola Superior do Ministério Público (FMP). (bernardo.teixeira93@edu.pucrs.br).

[2] Mestranda e graduanda em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). (laura.lino01@edu.pucrs.br).

Brazilian data protection legislation, known as "LGPD", has attributed significant relevance regarding the regulations on concent, as one of the bases for data processing, in order to demonstrate its concern with individual's participation in the flow of their information. Therefore, this present article aims to analyse consent inserted into the art. 7º of LGPD, as well as its historical aspects and its practical repercussions.
Keywords: Personal data protection. General Data Protection Law. Consent. Art. 7º.

INTRODUÇÃO:

O crescente impacto das novas tecnologias na vida em sociedade, verificado em décadas recentes, tem levado a um correspondente acréscimo na importância dos dados pessoais, os quais constituem, em larga medida, uma das principais mercadorias no atual estágio do capitalismo global. Disso resulta a necessidade de desenvolver mecanismos jurídicos adequados à tutela desses dados, tendo em vista sua intrínseca associação com o livre desenvolvimento de cada indivíduo e, em última instância, com a própria dignidade humana, valor máximo ao qual se reportam, direta ou indiretamente, todos os direitos fundamentais.

Nesse contexto, o direito à proteção de dados pessoais desenvolveu-se, inicialmente, em estrita associação com o direito fundamental à privacidade, historicamente amparado na dicotomia público-privado e centrado na liberdade negativa de não sofrer interferência alheia em sua esfera pessoal. Nessa esteira, com a evolução do conceito de privacidade, que não poderia mais ser limitado ao simples direito de ser deixado só, o direito à privacidade passaria a englobar o direito à proteção de dados pessoais, entendido como liberdade positiva de controle sobre as próprias informações.

No cenário europeu, a vinculação entre o direito à privacidade e a proteção de dados pessoais foi reconhecida em decisões da Corte Europeia de Direitos Humanos (CEDH) e do Tribunal de Justiça da União Europeia (TJUE), com base no artigo 8º da Convenção Europeia de Direitos Humanos, o qual trata do direito ao respeito da vida privada e familiar. Já no direito pátrio, anteriormente à aprovação da EC nº 115, entendia-se o direito fundamental à proteção de dados como implicitamente positivado, por meio da leitura harmônica da Constituição Federal, derivado ora do direito à privacidade, ora do direito (também implicitamente positivado) ao livre

desenvolvimento da personalidade, ou, ainda, do direito geral de liberdade ou do princípio da dignidade humana.

Em solo europeu, o direito à proteção de dados foi galgando o status de direito fundamental autônomo, como tal reconhecido em diversos documentos, iniciando pela Convenção nº 108 do Conselho Europeu (Convenção de Estrasburgo) e culminando na Carta de Direitos Fundamentais da União Europeia. Sua normatização, por sua vez, deu-se inicialmente através da Diretiva 95/46/CE, a qual deveria ser transposta para o direito interno dos países-membros. Atualmente, o sistema de proteção de dados da União Europeia encontra-se unificado em torno do Regulamento Geral de Proteção de Dados (GDPR), o qual é diretamente aplicável aos países integrantes do bloco.

No Brasil, ainda antes da promulgação da EC nº 115, que estabeleceu de forma autônoma o direito fundamental à proteção de dados pessoais, já estava em vigor a Lei Geral de Proteção de Dados (LGPD), em cujo texto estão estabelecidas as bases normativas para o tratamento de dados tanto pelo poder público quanto por particulares.

Dentre as bases normativas previstas na LGPD, mereceu especial destaque o consentimento do titular, o qual será objeto do presente trabalho. Assim, em um primeiro momento, abordar-se-á o desenvolvimento da proteção de dados como direito fundamental autônomo no sistema constitucional brasileiro; a seguir, tratar-se-á do conceito de dados pessoais adotado pela LGPD e da similaridade deste com o conceito estabelecido no GDPR; mais adiante, o foco serão as bases legais do tratamento de dados na LGPD, com ênfase no consentimento; por fim, serão tecidas algumas considerações à guisa de conclusão.

1. A PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL AUTÔNOMO

Em um contexto social de exponencial crescimento do setor da tecnologia, bem como de desenvolvimento dos meios de comunicação, sobrevém a gradual inserção de um processo de digitalização dos direitos fundamentais[3]. Atrelado a

---

[3] "Assim, não é à toa que já há tempos se fala em um processo de digitalização dos direitos fundamentais (ou de uma dimensão digital dos direitos fundamentais), bem como de uma

isso, observa-se, a partir dos avanços tecnológicos, que a disseminação de informações em larga escala acarreta diversas consequências à realidade dos cidadãos, entre elas o fenômeno de "*Ubiquituous Computing*", ou seja, a promoção do caráter de onipresença, fato que afeta e repercute em todas as esferas da vida social[4].

Perante essa realidade, caracterizada por uma "sociedade tecnológica"[5], é necessário considerar que, assim como no cotidiano fora da vida digital, os cidadãos são atingidos por violações aos seus direitos fundamentais, especialmente, àqueles inerentes aos titulares de dados, pois constantemente sofrem ataques ao ver sua privacidade e a sua intimidade infringidas, tal como ocorreu no emblemático caso da Cambridge Analytica em 2018[6].

Nesse sentido, torna-se imprescindível a utilização de instrumentos jurídicos que ambicionem à contenção dos riscos provocados pela chamada "datificação das coisas"[7].

Assim, a Lei Geral de Proteção de Dados, alicerçada de seu arcabouço legal que compõe o microssistema de proteção dos dados, ambicionou promover

---

digitalização do próprio direito (daí se falar também de um direito digital), o que, à evidência, inclui – mas de longe não só isso! – o reconhecimento gradual, na esfera constitucional e no âmbito do direito internacional, de um direito humano e fundamental à proteção de dados, assim como de outros princípios, direitos (e deveres) conexos, mas também de uma releitura de direitos fundamentais "clássicos"." SARLET, Ingo Wolfgang. (2020). **Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Revista Brasileira De Direitos Fundamentais. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 18 mar. 2023, p. 179-181.

[4] Id. **O direito fundamental à proteção de dados pessoais na constituição federal brasileira de 1988**. Privacy and data protection magazine - Revista científica na área jurídica n.º 1, 2021 (*on-line*). Disponível em:https://repositorio.pucrs.br/dspace/bitstream/10923/18868/2/O_Direito_Fundamental_Proteo_de_Dados_Pessoais_na_Constituio_Federal_Brasileira_de_1988.pdf. Acesso em: 25 mar. 2023, p. 4-5.

[5] "A proteção dos dados pessoais alcançou uma dimensão sem precedentes no âmbito da assim chamada sociedade tecnológica, notadamente a partir da introdução do uso da tecnologia da informática e da ampla digitalização que já assumiu um caráter onipresente e afeta todas as esferas da vida social, econômica, política e cultural contemporânea no mundo, fenômeno comumente designado de *Ubiquituous Computing*". Id. (2020). **Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Op cit., p. 179.

[6] Ibid.

[7] ALMEIDA, Juliana Evangelista de; LUGATI, Lys Nunes. **Da evolução das legislações sobre proteção de dados**: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito, [S. l.], v. 12, n. 02, p. 1–33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 18 mar. 2023, p. 2-3.

subsídios legais com vistas a disciplinar o tratamento dos dados pessoais, incluindo em seu escopo, inicialmente, fundamentos para tanto, conforme dispõem os artigos 1º [8] e 2º [9] da Lei.

Recentemente, o direito à proteção dos dados pessoais foi reconhecido como um direito fundamental[10] a partir da aprovação da PEC nº 17/2019, que incluiu no art. 5º da CF/88, com a Emenda Constitucional nº 115, o inciso LXXIX[11]. Antes dessa aprovação, o direito à proteção dos dados pessoais era implicitamente positivado, o que poderia ser observado a partir uma leitura harmônica e sistemática do texto constitucional[12].

2. LGPD E SUAS SIMILARIDADES COM O GDPR

Conforme dispõe em seu art. 5º, inciso I, a LGPD considera como dado pessoal toda "informação relacionada a pessoa natural identificada ou identificável" [13].

---

[8] Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm**. Acesso em: 25 mar. 2023.

[9] Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. Ibid.

[10] SARLET, Ingo Wolfgang. (2020). **Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Op cit.

[11] Art. 5º. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal, 1988. Disponível em: **https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.** Acesso em: 25 mar. 2023.

[12] Ibid, p. 184-186.

[13] BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm**. Acesso em: 03 jun. 2023.

Conforme destacam Viola e Teffé[14], tal definição ampla, baseada no pressuposto de que todo dado pessoal está investido de valor e importância, se aproxima daquela prevista pelo GDPR, que, em seu art. 4º, conceitua "dados pessoais" como sendo "informação relativa a uma pessoa singular identificada ou identificável"[15].

As similaridades, contudo, não se esgotam com a definição. Com efeito, assim como o GDPR buscou estabelecer hipóteses taxativas para o tratamento dos dados, devendo o controlador sempre enquadrar o tratamento realizado em uma delas, podendo, inclusive, cumulá-las, a mesma sistemática foi adotada pela LGPD[16]. No caso da legislação brasileira, as bases legais para o tratamento de dados se encontram dispostas no art. 7º[17] da LGPD, bem como em seu art. 11[18], este relativo

---

[14] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11, p. 115-146. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023.

[15] UNIÃO EUROPEIA. Regulamento (UE) no 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (**Regulamento Geral sobre a Proteção de Dados**). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: 2 jun. 2023.

[16] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11, p. 115-146. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023.

[17] Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm**. Acesso em: 03 jun. 2023.

[18] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas; II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307,

aos dados sensíveis[19], tratando-se, em ambos os casos, de rols taxativos, ainda que algumas hipóteses (e.g., a do legítimo interesse) contenham certo grau de subjetividade[20].

Da mesma forma, no que tange ao objeto central deste estudo, a definição de consentimento positivada no art. 5º, inciso XII, da LGPD ("manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada") dialoga com aquela estabelecida pelo legislador europeu, que o conceitua, em seu art 4º, nº 11, como "uma manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento"[21].

Partindo dessas definições, será abordado a seguir, de modo mais específico, o consentimento do titular como base legal para o tratamento de dados, buscando tornar mais clara a definição trazida pela LGDP, inclusive à luz de alguns documentos europeus, devido à já apontada similitude entre os conceitos.

---

de 23 de setembro de 1996 (Lei de Arbitragem); e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/20 20/lei/l14020.htm**. Acesso em: 03 jun. 2023.

[19] Definidos pelo art. 5º, inciso II, como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm**. Acesso em: 03 jun. 2023.

[20] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11, p. 115-146. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023.

[21] UNIÃO EUROPEIA. **Regulamento (UE) no 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE** (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: 02 jun. 2023.

3. CONSENTIMENTO DO TITULAR E AS BASES LEGAIS DO ART. 7º DA LGPD

Constata-se que a LGPD, em seu artigo 7º, conferiu especial destaque ao requisito do consentimento e trouxe a noção de que o consentimento do titular estaria atrelado ao princípio da autodeterminação informativa[22]. A relevância conferida à disciplina do consentimento se justifica devido à intensa disseminação de dados pessoais, conforme se observa na atualidade, que, à primeira vista, supostamente, podem não ser danosos aos seus titulares, pois diretamente não fazem referência a eles. Porém, esses dados, aparentemente genéricos, evidenciam informações que o identificam e, uma vez transferidos ou cruzados, podem revelar a identidade de seu titular, transparecendo inclusive dados de caráter sensível[23]. Um exemplo disso, foi o julgamento do caso sobre a lei do censo em 1983, julgado pelo Tribunal Constitucional Federal Alemão (*Bundesverfassungsgericht*)[24].

Embora não seja a única base legal estabelecida na LGPD para o tratamento de dados pessoais, nem tampouco esteja posicionada de forma hierarquicamente superior às demais hipóteses do art. 7º, percebe-se que o consentimento do titular dos dados recebeu atenção especial do legislador, o que demonstra sua preocupação com a participação do indivíduo no fluxo de suas informações[25].

Tal consentimento se fundamenta na possibilidade de autodeterminação da pessoa humana no que diz respeito aos seus dados pessoais, estando intimamente ligado à própria personalidade, sendo esse um fator que deve ser levado em consideração no momento de caracterizar a natureza jurídica e os efeitos desse consentimento[26].

---

[22] ALMEIDA, Juliana Evangelista de; LUGATI, Lys Nunes. **Da evolução das legislações sobre proteção de dados**: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Op cit., p. 2-3.

[23] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11, p. 131-162. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 131-132. (revista eletrônica).

[24] Ibid, p. 131.

[25] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, pp. 115-146.

[26] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 202, pp. 315-316.

De acordo com o art. 5º, inciso XII, da LGPD, o consentimento é caracterizado como "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*". Tal conceito, que dialoga com aquele estabelecido pelo legislador europeu na GDPR, deve ser interpretado de maneira restritiva[27], conforme será demonstrado a seguir.

Em primeiro lugar, a expressão *livre* significa que o titular dos dados pode optar por aceitar ou recusar o tratamento[28], sendo vedado expressamente, no art. 8º, inciso III, o tratamento mediante vício de consentimento.

Tais vícios podem se dar de várias formas, em especial aquelas previstas no Código Civil quanto aos negócios jurídicos, como erro (art. 138), dolo (art. 145), coação (art. 151), estado de perigo (art. 156), lesão (art. 157) e simulação (art. 167)[29].

Ainda, por estar diretamente relacionado à personalidade, que possui como um de seus atributos a indisponibilidade, o consentimento é passível de revogação incondicional pelo titular [30], mediante manifestação expressa, sendo que o tratamento realizado anteriormente será mantido até que seja requerida a eliminação dos dados pessoais. Além disso, importa ressaltar que a revogação do consentimento não implica, automaticamente, a interrupção do tratamento, haja vista a possibilidade de o controlador enquadrá-lo em outra base legal[31].

De outro giro, o consentimento deverá ser *informado*, i.e., o titular deverá ter consciência do destino dos seus dados pessoais, o que inclui informações quanto ao destinatário; à finalidade e duração do tratamento; quem terá acesso; se os dados poderão ser transmitidos a terceiros; além de outros detalhes que se façam necessários para formar a convicção livre e consciente do titular, possibilitando, assim, o exercício da sua autodeterminação[32].

---

[27] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 120.
[28] Ibid.
[29] OLIVEIRA, Márcio Cots Ricardo; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada.** 4. ed. São Paulo: Revista dos Tribunais, 2021, p. 99-101.
[30] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 202, p. 317.
[31] OLIVEIRA, Márcio Cots Ricardo; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada.** 4. ed. São Paulo: Revista dos Tribunais, 2021, p. 101.
[32] DONEDA, op. cit., p. 320.

Sobressai, aqui, a importância dos princípios da transparência, adequação e finalidade, a fim de minimizar as assimetrias técnica e informacional entre titular e controlador, bem como restringir a utilização genérica dos dados e a realização de tratamentos opacos. Assim, o titular deverá ser cientificado acerca dos riscos e implicações do tratamento dos seus dados[33].

Nesse ponto, verifica-se que o legislador estabeleceu como direito do titular "*o acesso facilitado às informações sobre o tratamento dos seus dados", informações essas que deverão ser disponibilizadas de forma clara, adequada e ostensiva"*. Considerando que a LGPD contempla o tratamento de dados tanto on-line como off-line, alguns autores consideram que tais informações devem ser disponibilizadas da mesma forma pela qual o tratamento de dados teve início. Assim, se o tratamento se iniciou através da internet, é por meio dela que as informações devem ser fornecidas; caso tenha se iniciado em lugar físico, é nele que o titular deverá acessar as informações[34].

Importante destacar que, caso sejam fornecidas ao titular informações de conteúdo enganoso ou abusivo, ou na hipótese de não terem sido apresentadas previamente, de modo transparente, claro e inequívoco, o consentimento fornecido será considerado nulo. Na mesma esteira, o controlador deverá informar ao titular caso ocorra alteração na finalidade do tratamento que seja incompatível com o consentimento inicial. Nessa hipótese, caso o titular não concorde com a mudança, este poderá revogar o consentimento[35].

Ainda, o consentimento deverá ser *inequívoco.* Por conseguinte, o consentimento não pode ser obtido por meio da omissão do titular, devendo sempre ser extraído a partir de atos que revelem claramente a sua vontade, seja por escrito ou por meio de um clique, por exemplo. A LGPD não impõe uma forma específica para o consentimento, mas caso esse seja obtido por escrito, deverá constar em cláusula destacada das demais disposições do contrato. Igualmente, encontra-se

[33] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 122.
[34] OLIVEIRA, Márcio Cots Ricardo; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 4. ed. São Paulo: Revista dos Tribunais, 2021, p. 105-6.
[35] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Op. cit., p. 122-3.

expressamente positivado na LGPD que caberá ao controlador o ônus de comprovar que o consentimento foi obtido de acordo com as disposições legais[36].

Também não se pode olvidar que a *finalidade* do tratamento deverá ser sempre informada previamente ao titular, tendo em vista o princípio da utilização não abusiva dos dados, bem como a recomendação de eliminação ou anonimização das informações que não sejam mais necessárias[37]

4. A MANIFESTAÇÃO LIVRE E O DESBALANCEAMENTO DO CONSENTIMENTO

Ao analisar o artigo 5º, XII da LGPD, que traz o conceito de consentimento, enquadrando-o como a "manifestação livre, informada e inequívoca", conforme abordado no tópico anterior, é fundamental, entretanto, pensar nas situações de desbalanceamento do consentimento, caso que haverá posição hierarquicamente superior ao titular dos dados pessoais. Tal circunstância pode interferir na obtenção do consentimento livre, por exemplo.

Gustavo Tepedino e Chiara Spadaccini de Teffé[38] entendem que a análise da assimetria na manifestação do consentimento se revela extremamente importante diante de eventual vulnerabilidade existente entre o controlador e o titular dos dados para se garantir que o consentimento ocorra de modo livre, informado e inequívoco. Sendo assim indispensável "verificar o "poder de barganha" do cidadão com relação ao tratamento dos dados pessoais, o que implica considerar quais são as opções do titular com relação ao tipo de dado coletado até os seus possíveis usos"[39]. Diante desse cenário, será fundamental conferir destaque ao artigo 18 da LGPD, que elenca direitos que podem ser utilizados para amparar o caso concreto.

A LGPD não traz uma disciplina específica que ampare essa situação, por isso é necessário realizar uma análise sistemática para com o GDPR, que contém

---

[36] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 123.

[37] VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Op. cit., p. 123.

[38] TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de dados pessoais na LGPD. p. 282-318. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.) et al. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thompson Reuters Brasil, 2020, p. 294-295.

[39] Ibid, p. 294.

arcabouço normativo direcionado a essa matéria. Nesse sentido, o GDPR, em seu considerando nº 43, aponta expressamente que "a fim de assegurar que o consentimento é dado de livre vontade, este não deverá constituir fundamento jurídico válido para o tratamento de dados pessoais em casos específicos em que exista um desequilíbrio manifesto (*imbalance of power*) entre o titular dos dados e o responsável pelo seu tratamento". Assim, diante de situação que cause hierarquia entre o controlador e o titular dos dados pessoais, será necessário que o titular dos dados escolha, de modo específico, a finalidade em relação ao tratamento dos dados, autorizando ou não, sendo inválido o consentimento caso não houver essa opção[40].

Além disso, a matéria possui respaldo no guideline nº 259/2017, o qual traz a hipótese de "desbalanceamento do consentimento". Essa normativa objetiva amparar a situação em que o controlador dos dados se encontra em posição hierarquicamente superior ao titular dos dados pessoais, o que poderia interferir na obtenção do consentimento livre.

5. DESAFIOS DA BASE LEGAL DO CONSENTIMENTO NO ÂMBITO DAS CRIANÇAS E DOS ADOLESCENTES

Não escapou ao legislador a necessidade de regular especificamente o tratamento de dados pessoais de crianças e adolescentes. Nesse sentido, já no *caput* do artigo 14[41], a LGPD estabelece o principal fundamento para esse tratamento, o qual deverá sempre observar o "melhor interesse" daqueles, de acordo com práticas que visem à promoção e à proteção de seus direitos fundamentais,

[40] É necessário pensar em situações, tal como as relações de trabalho, em que há um vínculo de empregador-empregado, pensando nas situações em que se perceba uma nítida uma dificuldade de sanar a assimetria existente nessa relação que cause hierarquia entre o controlador e o titular dos dados pessoais. Especificamente, no que tange às relações de trabalho e o ponto da manifestação de consentimento "livre", o GDPR possui o Working Party 29 (ou *Article* 29), sendo esse órgão consultivo europeu independente, que considera problemática a questão de os empregadores procederem ao tratamento de dados pessoais dos empregados com base no consentimento, uma vez que é questionável que esse consentimento seja dado espontaneamente. Dessa forma, não é recomendável a utilização da base legal do consentimento no âmbito das relações de trabalho, devido ao risco de não ser considerado válido.

[41] Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.

com absoluta prioridade, não podendo o controlador se valer de expedientes que violem ou explorem a vulnerabilidade infantojuvenil[42].

Ainda, o § 1º do artigo 14[43] dispõe sobre a necessidade de que um dos pais ou responsáveis legais pela criança consinta com o tratamento, de forma específica e destacada. Também nesse caso, o consentimento deverá ser livre, inequívoco e informado, bem como observar a sua finalidade. Ressalte-se que nem mesmo o consentimento parental será apto a validar o tratamento que não atenda ao melhor interesse das crianças e dos adolescentes[44].

Por sua vez, o § 2º[45] estabelece como obrigação do controlador dos dados de crianças manter públicas as informações sobre os tipos de dados coletados, além da prever a forma da utilização destes, bem como dos procedimentos para que o titular possa exercer os direitos previstos no artigo 18[46] da LGPD.

A regra acerca da necessidade do consentimento parental veio excepcionada no § 3º[47], o qual traz a possibilidade de tratamento de dados de crianças, por apenas uma vez e sem o armazenamento dos dados pessoais, com o objetivo estrito de contatar os pais ou o responsável legal ou para a proteção do titular, ficando vedado também o seu compartilhamento com terceiros.

---

[42] HENRIQUES, Isabela; PITA, Marina; HARTUNG, Pedro. A Proteção de Dados Pessoais de Crianças e Adolescentes. p. 201-227. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023.

[43] § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.

[44] HENRIQUES, Isabela; PITA, Marina; HARTUNG, Pedro. Op. cit. p. 213-214.

[45] § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.

[46] Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:
I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. (...)

[47] § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

Reiterando os princípios da finalidade, da adequação e da necessidade, o § 4º[48] determina que qualquer tratamento de dados de crianças, especialmente em se tratando de jogos e pela internet, deve se restringir ao mínimo necessário.

O § 5º[49] contém a determinação para que os controladores de dados pessoais implementem soluções técnicas, dentro dos esforços razoáveis, com o objetivo de garantir que os dados de criança somente serão tratados mediante prévio consentimento dos pais ou do responsável legal do titular, e não da criança diretamente.

Também não escapou das preocupações do legislador a eventual dificuldade da criança de ter plena compreensão sobre os limites do tratamento dos seus dados pessoais, quer em decorrência da natural falta de maturidade ou nível de conhecimento, ou de eventuais limitações físicas, auditivas, visuais ou mentais. Por isso, o § 6º[50] reforça a necessidade de clareza quanto à informação prévia ao tratamento dos dados, bem como a obrigação de implementar soluções de acessibilidade, cabendo observar oportunamente a Lei 13.146/2015 (Lei Brasileira de Inclusão da Pessoa com Deficiência - Estatuto da Pessoa com Deficiência), em especial, o disposto no artigo 63[51], que trata da obrigatoriedade de portais em geral implementarem soluções de acessibilidade.

Por fim, cumpre salientar que, embora a lei não mencione expressamente os adolescentes nos parágrafos do artigo 14, entende-se que eles também estão abarcados por essas hipóteses, na medida em que seria desprovido de sentido

---

[48] § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.

[49] § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

[50] § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança.

[51] Art. 63. É obrigatória a acessibilidade nos sítios da internet mantidos por empresas com sede ou representação comercial no País ou por órgãos de governo, para uso da pessoa com deficiência, garantindo-lhe acesso às informações disponíveis, conforme as melhores práticas e diretrizes de acessibilidade adotadas internacionalmente. (...).

privá-los de igual proteção, o que inclusive violaria as suas garantias constitucionais[52].

6. INSUFICIÊNCIAS DO CONSENTIMENTO

Não obstante a inegável importância do consentimento para o regime jurídico da proteção de dados, não se pode perder de vista o fato de que tal foco regulatório também revela algumas insuficiências em relação ao objetivo de assegurar ao titular um controle efetivo acerca do fluxo de seus dados pessoais. A esse respeito, Laura Mendes e Gabriel Fonseca[53] destacam três instâncias nas quais se sobressaem tais insuficiências: i) as limitações cognitivas do titular; ii) as situações nas quais não há verdadeira liberdade de escolha; e iii) as técnicas de tratamento e análise de dados a partir de *Big Data.*

A primeira dessas hipóteses diz com os pressupostos do consentimento informado, de acordo com os quais o titular dos dados, enquanto indivíduo capaz de agir racionalmente com vistas à maximização de seus interesses, poderá sopesar os custos e benefícios decorrentes de consentir ou não com determinado tratamento, desde que lhe sejam fornecidas informações suficientes para tanto. Tais pressupostos, contudo, são colocados em xeque a partir de evidências empíricas oriundas das ciências comportamentais, uma vez que as limitações cognitivas, como vieses e heurísticas, podem prejudicar a capacidade do titular de decidir de modo genuinamente racional acerca do fluxo de seus dados[54].

Já a segunda hipótese trata da vulnerabilidade do titular na relação contratual eletrônica, decorrente da assimetria de poder de barganha existente entre este e o controlador. Com efeito, a complexidade e abstração dos termos das políticas de privacidade, somados ao fato de que vários destes se baseiam no binômio "take it or leave it", sendo o custo de não consentir a impossibilidade de desfrutar do serviço

[52] HENRIQUES, Isabela; PITA, Marina; HARTUNG, Pedro. A Proteção de Dados Pessoais de Crianças e Adolescentes. p. 201-227. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 215.
[53] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. p. 73-94. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 81.
[54] Ibid, p. 79.

almejado, fazem com que o consentimento fornecido seja meramente aparente, uma vez que pode não refletir concretamente a autonomia decisória do titular[55].

Por sua vez, o terceiro caso tratado pelos autores está relacionado à utilização de grandes bancos de dados, cujo processamento, análise e cruzamento, por meio de modernas ferramentas, como algoritmos e inteligências artificiais, permite a extração de novas informações, inteiramente desconectadas da finalidade original para a qual os dados foram obtidos. Tais informações, por sua vez, além de seu potencial valor político-econômico, podem acarretar severos riscos à personalidade dos titulares dos dados, uma vez que os perfis virtuais criados a partir delas possuem o condão de influenciar decisões sobre emprego, moradia, crédito, entre diversas outras áreas que abrangem aspectos fundamentais da vida humana[56].

No entanto, o reconhecimento de tais insuficiências não implica o abandono do consentimento como instrumento regulatório, tampouco justifica a adoção de uma postura paternalista, no sentido de reduzir, à sua revelia, a liberdade do titular dos dados. Ao contrário, os autores buscam apaziguar tais insuficiências mediante instrumentos, conceitos e estratégias complementares que tornem o consentimento mais eficaz. São exploradas, então, três possibilidades: i) a proteção de dados através de meios tecnológicos; ii) a análise de risco e a criação de uma abordagem regulatória pautada pela ideia de *accountability;* e iii) a instituição de limites materiais ao consentimento[57].

No que tange à utilização da própria tecnologia para a proteção dos dados, importa destacar que o direito não é o único meio de regulação da internet, devendo ser conjugado com a tecnologia a fim de estabelecer condições que permitam a tomada de decisões verdadeiramente autônomas. Nesse contexto, é mister promover a criação de sistemas tecnológicos seguros e garantir a incorporação dos princípios que regem a proteção de dados não apenas nas leis e nos termos contratuais, mas também nos próprios sistemas tecnológicos utilizados para esse

[55] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. p. 73-94. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 81.
[56] Ibid.
[57] Ibid.

fim, com o intuito de promover a integração do conceito de autodeterminação informativa nos sistemas, códigos, arquiteturas e procedimentos tecnológicos[58].

Quanto à análise de risco e *accountability,* parte-se do pressuposto de que a responsabilidade pela proteção dos dados pessoais em um ambiente digital multifacetado não pode ser limitada apenas à gestão individual do titular, exclusivamente através de seu consentimento, mas deve ser compartilhada por todos os envolvidos, por meio da distribuição de responsabilidade e deveres de transparência entre eles, com foco especial no agente responsável pelo tratamento dos dados, seja ele público ou privado. Portanto, não basta atribuir direitos aos indivíduos, mas é fundamental estabelecer também condições institucionais para assegurá-los através da atuação conjunta dos diversos atores envolvidos, mediante a participação ativa na adoção de medidas preventivas de segurança, na formulação de estratégias de combate e redução dos riscos decorrentes de suas atividades, bem como na promoção de maior transparência ao conduzir esses procedimentos[59].

Por fim, importa considerar o contexto em que o consentimento e o tratamento dos dados se encontram inseridos, a fim de que os ideais de autonomia e de empoderamento individual não assumam uma dimensão meramente formal, mas que se obtenha um equilíbrio entre o consentimento e a finalidade do tratamento, levando-se em consideração a própria natureza dos dados. Nesse ponto, é possível valer-se de institutos civis já consolidados, como os relacionados aos vícios de vontade, abusos de poder ou cláusulas gerais como a boa-fé e a tutela da confiança, na busca pela concretização da autonomia e na análise do consentimento no contexto em que ocorre[60].

CONSIDERAÇÕES FINAIS

A manifestação do consentimento é, portanto, observada como elemento indissociável a ideia da proteção ao titular de dados pessoais, fato que se torna

---

[58] MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares da. Proteção de dados para além do consentimento: tendências de materialização. p. 73-94. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023, p. 81.
[59] Ibid.
[60] Ibid.

imprescindível de amparo legal, considerando o cenário de intensa disseminação de dados pessoais, inerente a atual sociedade globalizada. Dito isso, observou-se que a LGPD enfatizou a disciplina do consentimento, tendo como viés, a atuação do poder da autodeterminação informativa da pessoa, bem como considerando a aplicação dos direitos fundamentais em questão.

Dessa forma, como observado, o legislador conferiu especial destaque para a referida base legal, embora não sendo a única e nem a principal prevista no artigo 7º da LGPD. A importância conferida a base legal do consentimento decorre da necessidade de assegurar uma proteção ao titular dos dados, o que demonstra sua preocupação com a participação do indivíduo no fluxo de suas informações pessoais; logo, o consentimento pode ser observado como uma das formas de proteção dos dados pessoais ora amparada pela Lei Geral de Proteção dos Dados Pessoais.

Enfim, vislumbrou-se que a proteção de dados pessoais engloba temas não só relacionados ao direito à privacidade, mas também ampara funcionalidades dos valores fundamentais do ordenamento jurídico. Sendo assim uma ação positiva do Estado para atingir o patamar de isenção e de autoridade necessárias a um direito fundamental. Além do que, é reflexo de um perfil histórico, ora retratado, que remonta, agora, o direito fundamental autônomo expressamente positivado e amparado pela Carta Magna.

REFERÊNCIAS

ALMEIDA, Juliana Evangelista de; LUGATI, Lys Nunes. **Da evolução das legislações sobre proteção de dados**: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. Revista de Direito, [S. l.], v. 12, n. 2, p. 1–33, 2020. DOI: 10.32361/2020120210597. Disponível em: https://periodicos.ufv.br/revistadir/article/view/10597. Acesso em: 18/03/2023.

_____; _____. **A LGPD e a construção de uma cultura de proteção de dados**. Revista de Direito, Viçosa, v. 14, nº 1, 2022, p. 1–21, 2020. DOI: doi.org/10.32361/2022140113764. Disponível em: https://periodicos.ufv.br/revistadir/article/view/13764. Acesso em: 2 de mar. 2023.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 2 ed. Rio de Janeiro: Forense, 2020.

BRASIL. Constituição (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal: Centro Gráfico, 1988. Disponível em: **https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm.** Acesso em: 25/03/2023.

_____. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, (2020). Disponível em: **https://www.planalto.gov.br/ccivil_03/_ato2019-20
22/2020/lei/l14020.htm.** Acesso em: 25/03/2023.

BORLLI, Alessandra. O tratamento de dados de crianças no âmbito do General Data Protection Regulation (GDPR). p. 135-161. *In.* NOBREGA, Viviane; BLUM, Renato Opice (coord.) et al. **Comentários ao GDPR**: regulamento geral de proteção de dados da União Europeia. 2 ed. São Paulo: Thompson Reuters Brasil, 2019.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: fundamentos da Lei Geral de Proteção de Dados. 3. ed. São Paulo: Revista dos Tribunais, 202.

LIMA, Caio César Carvalho. Do tratamento de dados pessoais. p.179-214. *In.* NOBREGA, Viviane; BLUM, Renato Opice (coord.) et al. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thompson Reuters Brasil, 2019.

NOBREGA, Viviane Maldonado. Dos direitos do titular. P. 220-242. *In.* NOBREGA, Viviane; BLUM, Renato Opice (coord.) et al. **LGPD**: Lei Geral de Proteção de Dados comentada. 2. ed. rev., atual. e ampl. São Paulo: Thompson Reuters Brasil, 2019.

OLIVEIRA, Márcio Cots Ricardo; OLIVEIRA, Ricardo. **Lei geral de proteção de dados pessoais comentada**. 4. ed. São Paulo: Revista dos Tribunais, 2021.

RODOTÁ, Stefano. **A vida na sociedade de vigilância** – a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo Wolfgang. (2020). **Proteção de dados pessoais como direito fundamental na constituição federal brasileira de 1988**: contributo para a construção de uma dogmática constitucionalmente adequada. Revista Brasileira De Direitos Fundamentais. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/875. Acesso em: 18/03/2023.

_____. **O direito fundamental à proteção de dados pessoais na constituição federal brasileira de 1988.** Privacy and data protection magazine - Revista científica na área jurídica n.º 1, 2021 (*on-line*). Disponível em: https://repositorio.pucrs.br/dspace/
bitstream/10923/18868/2/O_Direito_Fundamental_Proteo_de_Dados_Pessoais_na_Constituio_Federal_Brasileira_de_1988.pdf. Acesso em: 25/03/2023.

TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. Consentimento e proteção de

dados pessoais na LGPD. p. 282-318. *In*: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (coord.) et al. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. 2. ed. São Paulo: Thompson Reuters Brasil, 2020.

VAINZOF, Rony. Dados pessoais, tratamento e princípios. *In.* NÓBREGA, Viviane; BLUM, Renato Opice (coord.) et al. **Comentários ao GDPR**: regulamento geral de proteção de dados da União Europeia. 2 ed. São Paulo: Thompson Reuters Brasil, 2019.

VIOLA, Mario; TEFFÉ, Chiara Spadaccini de. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais dos artigos 7º e 11. *In*: MENDES, Laura Schertel Ferreira (coord) et al. **Tratado de proteção de dados pessoais.** 2 ed. Rio de Janeiro: Forense, 2023.

3. LIBERDADE DE EXPRESSÃO E MODERAÇÃO DE CONTEÚDO EM REDES SOCIAIS: *SHADOW BANNING*

https://doi.org/10.36592/9786554600712-03

Fabrizio Predebon da Silva[1]

SUMÁRIO

1 Introdução; 2 Liberdade de Expressão na Era Digital; 3 Moderação de Conteúdo por Meio de Algoritmos; 3.1 Dados e Perfilização; 3.2 Moderação e Curadoria de Conteúdo; 3.3 *Shadow Banning*; 4 Regramento Atual e Perspectivas; 5 Considerações Finais.

RESUMO

A criação de redes sociais e a evolução da tecnologia da informação e comunicação mudaram a forma como as pessoas se comunicam, recebem e difundem informações, além de ter ampliado o potencial exercício da liberdade de expressão dos usuários. O sucesso do modelo de negócios dessas plataformas digitais passa pela obtenção, tratamento e utilização de dados pessoais, especialmente para as atividades de moderação de conteúdo com fins de aumento de engajamento do usuário e de direcionamento de publicidade. Diante desse cenário, este trabalho buscou avaliar se a redução de conteúdo, e mais especificamente o *shaddow banning*, influenciam o exercício da liberdade de expressão, e se há regramento posto ou em discussão no Congresso Nacional para tratar do tema. Como resultado, concluiu-se que a ausência de normativa quanto à moderação de conteúdo pode impactar negativamente na liberdade de expressão, além de impossibilitar a aferição da legitimidade constitucional da aplicação das técnicas pelas redes sociais.
Palavras-chave: Liberdade de expressão; redes sociais; moderação de conteúdo; redução de visibilidade; *shaddow banning.*

ABSTRACT

The creation of social networks and the evolution of information and communication technology has changed the way people communicate, receive and disseminate information, and expanded the potential exercise of freedom of expression by users. The success of the business model of these digital platforms involves obtaining, processing and using personal data, especially for content moderation activities with the aim of increasing user engagement and targeting advertising. In view of this scenario, this study sought to assess whether content reduction, and more specifically shadow banning, influence the exercise of freedom of expression, and

[1] Mestrando no curso de pós-graduação em Direito na Pontifícia Universidade Católica do Rio Grande do Sul. Procurador da República. E-mail: fabrizio.silva@edu.pucrs.br

whether there is a rule in place or under discussion in the National Congress to address the issue. As a result, it was concluded that the absence of regulations regarding content moderation can negatively impact freedom of expression, in addition to making it impossible to assess the constitutional legitimacy of the application of the technique by social networks.
Keywords: Freedom of expression; social media; content moderation; visibility reduction; shadow banning.

1 INTRODUÇÃO

A liberdade de expressão ganhou novas formas de exercício a partir do desenvolvimento da internet, com destaque para as redes sociais, fenômeno que conectou bilhões de pessoas ao redor do mundo, entregando mensagens e publicações de forma instantânea e possibilitando que o conteúdo alcance ampla visibilidade. Superou-se a versão da mídia tradicional, representada apenas pela televisão, jornal, revista e rádio, que tinha vários *gatekeepers* e poucos publicadores, com a ascensão da mídia social, caracterizada por pouquíssimos *gakekeepers*, a exemplo do Facebook, Twitter, Instagram e Tik Tok, e muitos publicadores em potencial: os usuários.

Quem organiza a enorme quantidade de conteúdo publicado nas mídias sociais são os intermediários, as redes sociais e plataformas digitais, com base em regras por elas desenvolvidas. Por meio da moderação de conteúdo, elas avaliam o que está de acordo com os termos de uso, o que será entregue para cada um e o que ou quem terá a visibilidade ampliada ou reduzida, fato que demonstra inegável potencial de controle por entes privados sobre o exercício da liberdade de expressão *online*. E uma modalidade particular de moderação, o *shadow banning*, é especialmente preocupante, considerando a dificuldade de sua detecção.

Tendo por base o cenário exposto, este trabalho procura responder às seguintes perguntas: o *shadow banning* pode afetar o exercício da liberdade de expressão? Há regramento no ordenamento jurídico brasileiro aplicável ao caso? Quais as perspectivas de avanço legislativo acerca da temática?

Para alcançar as respostas, será utilizado o método de abordagem sistêmico, analisando-se a relação entre a liberdade de expressão e a moderação de conteúdo,

bem como o regramento aplicável, caso existente. Em relação aos métodos de procedimento, será utilizado o histórico, investigando-se a mudança por que passou o exercício da liberdade de expressão. Já quanto ao método interpretativo, utilizar-se-á o sociológico, considerando-se o Direito como ferramenta para regular a interação social e assegurar a liberdade de expressão. Por fim, o tipo de pesquisa adotado será bibliográfico.

O texto será estruturado em três tópicos. O tópico 2 abordará a liberdade de expressão na era digital a partir do desenvolvimento da mídia social. O tópico 3 tratará da moderação de conteúdo no âmbito das plataformas digitais, adentrando nas temáticas relativas a tratamento de dados, perfilização e *shadow banning*. O tópico 3 investigará a legislação atual aplicável ao *shadow banning*, bem como as perspectivas legislativas para a temática.

2 LIBERDADE DE EXPRESSÃO NA ERA DIGITAL

Na era das comunicações em massa, a distribuição e o consumo de informações, notícias e opiniões migrou em grande parte das mídias tradicionais para a mídia social. Conforme pesquisa realizada pelo Instituto Reuters em 46 países no ano de 2023, ao buscar notícias *online*, 30% dos entrevistados o fazem por meio de redes sociais, enquanto 22% acessam diretamente os sites ou plataformas das mídias tradicionais. Em 2018, esses números eram de 22% pelas mídias sociais e 32% diretamente pelos canais *online* das mídias tradicionais[2]. Já de acordo com outra pesquisa, realizada pela Kaspersky no ano de 2021, 71% dos internautas brasileiros entrevistados afirmaram ter se informado por meio das redes sociais nos 12 meses anteriores, enquanto 83% dos entrevistados afirmaram cuidar da saúde com base em informações compartilhadas em redes sociais[3].

---

[2] DE LUCA, Aldo. Pesquisa do Instituto Reuters em 46 países confirma poder das mídias sociais como fonte de notícias. **Media Talks**, 2023. Disponível em: https://mediatalks.uol.com.br/2023/06/14/pesquisa-mostra-poder-das-midias-sociais-para-acesso-a-noticias-no-mundo/. Acesso em: 24/07/2023.

[3] BRANCO, Dácio Castelo. 7 em cada 10 brasileiros se informa por redes sociais — e isso afeta a segurança. **Canaltech**, 2021. Disponível em: https://canaltech.com.br/seguranca/7-em-cada-10-brasileiros-se-informa-por-redes-sociais-e-isso-afeta-a-seguranca-198668/. Acesso em: 12/05/2023. A pesquisa mencionada é intitulada "a infodemia e os impactos na vida digital",

As redes sociais, expressão do avanço da tecnologia da informação e da comunicação, permitem que os usuários fiquem permanentemente conectados no ambiente virtual e divulguem ideias e informações com potencial para alcançar o mundo inteiro, em superação das barreiras geográficas e da relativa exclusividade de publicação nos meios convencionais de imprensa. De acordo com Zuboff:

> [a]s necessidades individuais de auto-expressão, voz, influência, informação, aprendizado, empoderamento e conexão convocaram todos os tipos de novos recursos à existência em apenas alguns anos: pesquisas do Google, música do iPod, páginas do Facebook, vídeos do YouTube, blogs, redes, comunidades de amigos, estranhos e colegas, todos alcançando além dos antigos limites institucionais e geográficos em uma espécie de exultação de caça, coleta e compartilhamento de informações para todos os propósitos ou para nenhum.[4,p.79]

A partir dessa perspectiva, em um primeiro momento, é possível afirmar que houve a popularização do direito de publicação e a democratização do acesso à informação, em processo com imenso potencial de fortalecimento dos regimes democráticos. Com efeito, algumas das mais significativas lutas pelos direitos humanos são travadas nas redes digitais[5], ou organizadas por meio dela, a exemplo da *People's climate march*, que reuniu mais de 300.000 pessoas em Nova York em setembro de 2014, que seria palco de encontro de líderes das Nações Unidas para discussão sobre mudanças climáticas, para pressionar as autoridades a adotar medidas preventivas[6].

A maximização ou potencialização da liberdade de expressão pelas plataformas digitais pode enriquecer o debate público no ambiente virtual com a

---

disponível mediante solicitação em https://www.kaspersky.com.br/blog/pesquisa-infodemia-impactos-vida-digital/17467/.

[4] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89. Tradução livre.

[5] BUSTAMANTE, Javier. Poder comunicativo, ecossistemas digitais e cidadania digital. In: SILVEIRA, Sergio Amadeu da. **Cidadania e Redes Digitais.** 1ª Edição. São Paulo: Maracá – Educação e Tecnologias, 2010.

[6] FODERARO, Lisa W. Taking a Call for Climate Change to the Streets. **The New York Times**, 2014. Disponível em: https://www.nytimes.com/2014/09/22/nyregion/new-york-city-climate-change-march.html. Acesso em: 25/07/2023.

participação de mais atores e a partir da convivência das diferentes visões de mundo ali manifestadas, que contribuem para a formação do pensamento a partir da contraposição de ideias[7, p. 403]. Trata-se da democratização e da diversificação do mercado da informação a partir da evolução da tecnologia da informação e comunicação[8, p. 1833]. E mais, o incremento da troca de informações pelo ciberespaço facilita a formação coletiva do conhecimento e a difusão da cultura, além de permitir maior inclusão na formação da opinião pública e no controle dos atos públicos, em profundo exercício da participação política a que Javier Bustamante dá o nome de *hipercidadania* ou *cidadania digital*[9, p. 17].

Apesar dos potenciais benefícios mencionados em caráter exemplificativo, a ampliação da interação humana no mundo digital também tem como consequência o aumento dos conflitos de direitos fundamentais, aqui destacando-se a liberdade de expressão. Se há mais pessoas exercendo tal liberdade, há também mais possibilidades de extrapolação de seus limites constitucionais. Da perspectiva do Direito, importa debater formas pelas quais é possível equilibrar a potencializada liberdade de expressão com outros direitos e princípios de estatura constitucional.

As redes sociais e plataformas digitais são os principais responsáveis pela transformação da comunicação social e pela ascensão e consolidação da mídia social, hoje o meio mais efetivo de propagação de opiniões e pensamentos[10, p.87]. Soma-se à ampliação do número de comunicadores, que contribui para o pluralismo das fontes, e à ampliação do acesso à informação, aqui visto como o direito de se informar, o incremento da pluralidade dos meios de comunicação, fatores decisivos na promoção da liberdade de expressão e do direito à informação na era digital.

Em 1995, Eugene Volokh afirmou que a mídia, referindo-se aos jornais, às revistas e às estações de rádio e de televisão, controlavam quais comentadores

---

[7] FREDES, Andrei Ferreira. Liberdade de expressão e configuração do ambiente virtual: o controle do fluxo de informação e expressão na internet. In: SARLET, Ingo Wolfgang; RUARO, Regina Linden; LEAL, Augusto Antônio Fontanive (orgs.). **Direito, Ambiente e Tecnologia: estudos em homenagem ao professor Carlos Alberto Molinaro**. Porto Alegre: Fundação Fênix, 2021. p. 401-423.

[8] VOLOKH, Eugene. Cheap speech and what it will do. **Yale LJ**, v. 104, 1994, p. 1805-1850.

[9] BUSTAMANTE, Javier. Poder comunicativo, ecossistemas digitais e cidadania digital. In: SILVEIRA, Sergio Amadeu da. **Cidadania e Redes Digitais**. 1ª Edição. São Paulo: Maracá – Educação e Tecnologias, 2010.

[10] SARLET, Ingo Wolfgang; HARTMANN, Ivar. Direitos fundamentais e direito privado: a proteção da liberdade de expressão nas mídias sociais. **RDU**, Porto Alegre, Volume 16, n. 90, 2019, p. 85-108.

estariam disponíveis para acesso ao público, sendo esse controle baseado em suas opiniões políticas e no que os consumidores das informações possivelmente gostariam de receber.[11, p. 22] Seguiu a autora sustentando que o avanço da tecnologia e o baixo custo da distribuição eletrônica tenderiam a retirar o controle da circulação de informação exercido pelos intermediários e repassá-lo aos comunicadores, liberando-os da necessidade de satisfazer os intermediários para poder falar. Tais avanços, segundo a autora, também dariam aos consumidores das informações maior controle do que seria consumido.[12, p. 1834]

De acordo com a previsão de Volokh, os intermediários seriam suprimidos da cadeia de distribuição das informações, permitindo-se maior participação do público na produção e distribuição de conteúdo. A autora acertou em vários pontos, e de fato foram potencializados a liberdade de expressão e o direito à informação, porém ela não anteviu, e nem teria como, o desenvolvimento do “capitalismo de vigilância"[13], que tornou os novos intermediários muito mais poderoso do que os anteriores. Esse poder advém da concentração de mercado de poucas grandes empresas de tecnologia, alcançado através do sucesso na obtenção, processamento e utilização de dados pessoais para, ao mesmo tempo, maximizar a experiência do usuário e tornar a publicidade mais eficiente.

Os novos intermediários, as redes sociais e outras plataformas digitais, como o Youtube, antes vistos como simples hospedeiros de conteúdo, têm atuação central na perfilização dos usuários e na classificação de conteúdo, de forma a distribuí-lo sob medida para aumentar ou manter o engajamento, ou a suprimi-lo nos casos de violação dos termos e condições de uso da plataforma. Há, então, influência direta das companhias gerenciadoras de tais plataformas no exercício da liberdade de expressão e do direito à informação, como se verá no tópico seguinte.

---

[9] VOLOKH, Eugene. Cheap speech and what it will do. **Yale LJ**, v. 104, 1994, p. 1805-1850.
[12] *Ibidem*.
[13] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89.

3 MODERAÇÃO DE CONTEÚDO POR MEIO DE ALGORITMOS

A multiplicação do número de publicadores e a facilidade de publicação proporcionadas pelas redes sociais tiveram por consequência lógica o aumento exponencial do conteúdo disponível *online* em proporções jamais vistas. Para se ter ideia, em 2021, a cada minuto, 350 mil tweets foram publicados no Twitter (agora denominado X) e 510 mil comentários foram publicados no Facebook[14]. Em junho de 2022, a cada minuto, 500 horas de vídeo foram carregadas para o Youtube[15]. Em 2023, estima-se que haja 4,8 bilhões de usuários espalhados em todas as redes sociais, e que o Facebook e o YouTube têm 2,96 bilhões e 2,52 bilhões de usuários ativos por mês, respectivamente[16].

Essa grande quantidade de conteúdo deve ser organizada de alguma forma para ser apresentada aos usuários, seja por data de *upload* ou por relevância. Aí que entra a governança exercida pelas empresas gerenciadoras das plataformas: a moderação de conteúdo e a recomendação algorítmica[17]. Já quanto aos bilhões de usuários, estes devem ser perfilizados e categorizados para receberem o conteúdo ou a recomendação de conteúdo correspondente ao seu enquadramento.

3.1 Dados e perfilização

O desenvolvimento tecnológico permitiu que alcançássemos a era do *big data*, embora este não seja consectário lógico daquele. Para Zuboff, "'big data' é, acima de tudo, o componente fundante em uma nova lógica de acumulação profundamente

---

[14] CHAFFEY, Dave. What happens online in 60 seconds in 2021? **Smart Insights**, 2021. Disponível em: https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/. Acesso em: 26/07/2023.

[15] Hours of video uploaded to YouTube every minute as of February 2022. **Statista**, 2023. Disponível em: https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/. Acesso em: 26/07/2023.

[16] CHAFFEY, Dave. Global social media statistics research summary 2023. **Smart Insights**, 2023. Disponível em: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/. Acesso em: 26/07/2023. De acordo com a pesquisa, o número de usuários pode não representar o número de indivíduos únicos que acessam as várias redes sociais, considerando que alguns acessam mais de uma, e que há contas operadas por *bots*.

[17] GILLESPIE, Tarleton. Do not recommend? Reduction as a form of content moderation. **Social Media+ Society**, v. 8, n. 3, julho-setembro, 2022. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/20563051221117552. Acesso em: 27/07/2023.

intencional e altamente consequente" que ela chama de capitalismo de vigilância, em que se busca "prever e modificar o comportamento humano como meio de produção de lucros e controle de mercado" [18, p. 75]. E o que se acumula? O capitalismo do século XXI centrou-se na extração e uso de dados[19, p. 28], o que foi possibilitado em grande parte pelo barateamento do custo da tecnologia necessária para transformar atividades em dados, assim como pela digitalização das comunicações[20, p. 28].

Big data, assim, constitui-se "pela captura de pequenos dados das ações e declarações mediadas por computador dos indivíduos em sua busca por uma vida efetiva".[21, p. 79] Toda e qualquer ação realizada em plataformas digitais pode ser transformada em dados e capturada. "Nada é muito trivial ou efêmero para essa colheita: 'curtidas' no Facebook, pesquisas no Google, e-mails, textos, fotos, músicas e vídeos, localização, padrões de comunicação, redes, compras, movimentos, cada clique, palavra com erro ortográfico, visualização de página e mais."[22, p. 79]

De acordo com Srnicek, os dados passaram a ocupar papel central na economia, servindo a diversas funções capitalistas:

> "eles educam e dão vantagem competitiva aos algoritmos; permitem a coordenação e terceirização de trabalhadores; permitem a otimização e flexibilidade dos processos produtivos; possibilitam a transformação de bens de baixa margem em serviços de alta margem; e a própria análise de dados é geradora de dados, em um ciclo virtuoso."[23, p. 29]

Mas dados, apenas, não são suficientes para prever ou influenciar o comportamento humano, ou para simplesmente possibilitar à plataforma a entrega ou recomendação ao usuário de conteúdo ou anúncio publicitário de seu interesse. Esses dados brutos são refinados, analisados, organizados e transformados em

---

[18] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89. Tradução livre

[19] SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press. 2017.

[20] *Ibidem.*

[21] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89. Tradução livre

[22] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89. Tradução livre

[23] SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press. 2017. Tradução livre.

mais dados ou informações para poderem ser usados. Quanto mais interação do usuário, mais dados são obtidos e mais precisa é a análise. Trata-se a análise de tarefa mais cara e complexa, realizada por "cientistas de dados ou por trabalho automatizado de algoritmos de *machine learning*"[24, p. 32]. Esses dados ainda podem ser cruzados com outros bancos de dados, que digam respeito, por exemplo, à renda familiar, ao local de trabalho, ao tempo que falta para a aposentadoria, à margem consignável restante no contracheque. O número das diferentes possibilidades de uso dos dados é diretamente proporcional à quantia de dados que se tem acesso[25,p.28].

Com base na análise dos dados, a plataforma avalia e encaixa cada usuário em determinado perfil[26], avaliando e prevendo aspectos relativos à sua vida pessoal, como predisposições, gostos, desgostos, capacidades, interesses, comportamentos, atividades, ou seja, analisa-se absolutamente tudo que for possível a depender dos dados obtidos e da ciência empregada. Os dados são capturados, adquiridos, vendidos, analisados e reanalisados, em processo denominado *data exhaust*[27, p. 79].

A partir da segmentação dos usuários em perfis, "os anunciantes podem direcionar anúncios publicitários ou customizar a experiência do usuário de maneira que (eles esperam) otimize o comportamento de compras"[28, p. 30]. Se muitos vendedores perceberam essa possibilidade, foi o Google que, pensando além, encontrou uma forma de financiar seus negócios *online* transformando os dados coletados em direcionamento de anúncios publicitários por meio da ferramenta Google AdWords[29, p. 24], hoje, Google Ads. Em 2022, os ganhos do Google com

---

[24] *Ibidem*.
[25] *Ibidem*.
[26] O artigo 4º, (4), do Regulamento Geral Sobre a Proteção de Dados da União Europeia, define *profiling* nos seguintes termos: "*'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;*"
[27] ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v. 30, n. 1, 2015, p. 75-89.
[28] WEST, Sarah Myers. Data capitalism: Redefining the logics of surveillance and privacy. **Business & society**, v. 58, n. 1, 2019, p. 20-41. Tradução livre.
[29] *Ibidem*.

anúncios publicitários totalizaram 224,47 bilhões de dólares, o que correspondeu a 79% dos ganhos da empresa.[30]

A mudança do modelo de comércio eletrônico (*dotcom business*), baseado na venda *online* de bens, para o modelo de anúncios publicitários, baseado na venda de audiências e de perfis individuais comportamentais, é parte do que West denomina *data capitalism*, "um sistema em que a comoditização de nossos dados permite a redistribuição de poder na era da informação".[31, p. 23] O poder passa para os atores com capacidade de entender e explorar a massiva quantidade de dados produzida diariamente por usuários de aplicativos ou dispositivos aptos a transformar em dados as atividades por meio dele desenvolvidas.

Srnicek, por sua vez, identifica que esse novo modelo de negócios é exercido por um novo tipo de empreendimento, a plataforma, em um sistema econômico que ele dá o nome de *platform capitalism*. Segundo o autor, as plataformas "tornaram-se uma maneira eficiente de monopolizar, extrair, analisar e usar as crescentes quantidades de dados que eram armazenados".[32, p 29].

Após o enquadramento dos usuários em perfis, as plataformas podem apresentar ou recomendar conteúdo sob medida, privilegiando aqueles que tendem a gerar mais tempo e atos de interação, além de direcionar publicidade com mais precisão, tornando os atos publicitários mais eficientes com a identificação do público-alvo.

3.2 Moderação e curadoria de conteúdo

As redes sociais são plataformas que conectam pessoas e hospedam conteúdo gerado por usuários. Os novos intermediários, diferentemente das emissoras de rádio e televisão, dos jornais e das revistas, não são produtores de conteúdo, mas moderadores, que têm sua razão de ser na publicação alheia e no

---

[30] CUOFANO, Gennaro. How Much Money does Google make from advertising? **FourWeekMBA**, 2023. Disponível em: https://fourweekmba.com/how-much-money-does-google-make-from-advertising/. Acesso em: 28/07/2023.

[31] WEST, Sarah Myers. Data capitalism: Redefining the logics of surveillance and privacy. **Business & society**, v. 58, n. 1, 2019, p. 20-41. Tradução livre.

[32] SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press. 2017. Tradução livre

tráfego de usuários. Portanto, a organização do ambiente (a governança) é chave para o sucesso.

Essas plataformas assumem um importante papel cívico, na medida em que as pessoas dependem cada vez mais delas para a obtenção de notícias e informações. [33, p. 139] E como visto, a quantidade de informações e conteúdo publicados é enorme, tendo as redes sociais desenvolvido algoritmos para eventualmente avaliar o cumprimento das regras da plataforma e para filtrar, organizar, ranquear e distribuir o conteúdo de forma personalizada aos usuários. A moderação de conteúdo, assim, consiste no "conjunto de normas e práticas (também compreendido como *sociotechnical desing*) adotadas pela mídia social que tornam o conteúdo acessível ou inacessível" [34]. Tais procedimentos são de natureza autorregulatória, fator que estimula que seu impacto nos negócios seja mais determinante para a sua elaboração e execução do que o impacto causado nos direitos fundamentais dos usuários[35, p. 3].

O ato de controle sobre o que pode ser publicado, que pode resultar na exclusão da publicação pela plataforma, e que tem por base o cumprimento das regras do ambiente, é parte do que se denomina moderação de conteúdo. O espaço virtual disponibilizado é privado, e conta com regras de convivência dispostas nos termos e condições de uso, de observância obrigatória. Dentre os principais motivos para o regramento e controle estão a prevenção dos intermediários contra processos por manutenção de conteúdo ilegal e contra a transformação do ambiente em um local de práticas agressivas ou abusivas que afastem os usuários. [36, p. 144]

Essa primeira modalidade de moderação é identificada por York e Zuckerman como *hard control*[37, p. 140]. Trata-se de ato aparentemente mais invasivo praticado

---

[33] YORK, Jillian C.; ZUCKERMAN, Ethan. Moderating the public sphere. In Jørgensen, R. F. (Ed.), **Human rights in the age of platforms**, v. 137, 2019, p. 137-161.

[34] MARONI, Marta. 'Mediated transparency': The Digital Services Act and the legitimisation of platform power. Publicado em abril de 2023. In LEINO-SANDBERG , Päivi; HILLEBRANDT, Maarten Zbigniew; KOIVISTO, Ida (editores). **(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice.** Editora Routledge. Livro ainda não publicado. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4413531. Acesso em: 31/07/2023.

[35] LEISER, M. R. Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News, Disinformation, & Online Manipulation. Data da publicação: maio de 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4427493. Acesso em: 01/08/2023.

[36] YORK, Jillian C.; ZUCKERMAN, Ethan. Moderating the public sphere. In Jørgensen, R. F. (Ed.), **Human rights in the age of platforms**, v. 137, 2019, p. 137-161.

[37] *Ibidem*.

por ator privado e que pode gerar consequências no exercício da liberdade de expressão, seja pela exclusão de publicação ou pela inibição ou desencorajamento decorrente do receio de punição, que pode ser executada tanto pela exclusão do conteúdo como pela suspensão ou banimento do usuário da plataforma. A exclusão de publicação (considerada em abstrato) significa o silenciamento, a supressão de uma manifestação, portanto a interferência no gozo de um direito fundamental. Já a suspensão e o banimento significam o impedimento temporário ou definitivo do exercício da liberdade de expressão e do direito à informação em determinado ambiente virtual. Vale ressaltar que a posição monopolista alcançada por determinadas plataformas torna a suspensão e o banimento ainda mais gravosos, considerando que nem sempre há substitutibilidade entre as redes sociais.

A exclusão de conteúdo é indiscutivelmente importante para o respeito dos direitos fundamentais, nos casos em que realizada para promover direitos e princípios constitucionais. O grande desafio é a identificação da legitimidade constitucional da supressão da liberdade de expressão em cada caso concreto. Quando a exclusão reforça o sistema de direitos fundamentais e quando ela é considerada censura? Já a suspensão e o banimento são ainda mais polêmicos, pois impedem temporária ou permanentemente o trânsito de usuários em espaços em que ocorrem debates públicos, fato que atinge também o direito de acesso à informação. São temas instigantes, mas que fogem do escopo deste trabalho.

Uma outra modalidade de moderação do conteúdo, denominada *soft control*, consiste na "autoridade da plataforma sobre o que provavelmente veremos, e o que é preterido pelos algoritmos que governam a visão do usuário sobre as postagens na rede (o *feed*)"[38, p. 140]. Essa intervenção é menos explícita do que o *hard control*, exercendo influência mais discreta, mas não menos importante, no exercício da liberdade de expressão e no direito à informação.

Aqui entra a recomendação algorítmica, que tem a função de entregar o conteúdo sob medida para cada usuário, com a finalidade de manter ou aumentar o engajamento, o que possibilita mais coleta de dados e mais público para a entrega

---

[38] *Ibidem*. Tradução livre.

de anúncios publicitários, em um ciclo sem fim que torna as recomendações cada vez mais precisas à medida que a base de dados das plataformas aumenta.

A recomendação algorítmica exerce papel fundamental na formação da opinião pública, uma vez que é responsável por praticamente todo o conteúdo que é consumido passivamente pelos usuários, aí incluídas notícias e opiniões, assim como desinformação e discursos de ódio. Nesse ponto também não restam dúvidas sobre a grande influência que os modelos de negócios das plataformas têm sobre o exercício da liberdade de expressão e do direito à informação.

Por fim, a forma de moderação de conteúdo mais difícil de ser notada pelos usuários é a redução de visibilidade de publicação ou de usuário, assunto objeto do subtópico seguinte.

3.3 *Shadow Banning*

Os poderes das redes sociais sobre a propagação de conteúdo publicado por usuários são enormes. É inegável que os algoritmos desenvolvidos têm a capacidade de maximizar a experiência dos usuários e manter a sua atenção à plataforma por mais tempo a partir da entrega ou recomendação de conteúdo sob medida. Inclusive a isso já se deu o nome de *attention economy*[39, p. 27]. Também é de conhecimento comum que, para fins de engajamento, os algoritmos maximizam a visualização de determinados conteúdos ou publicações. Esse é um ponto central do modelo de negócios das plataformas de publicidade: sediar atividades dos usuários, transformar todas as atividades realizadas na plataforma (e fora dela, por vezes) em dados, refiná-los e usá-los das mais variadas formas[40, p. 35], monetizando o negócio a partir de anúncios publicitários.

Se os algoritmos podem maximizar a visibilidade, eles também podem ser programados para reduzir a visibilidade de publicações, e se isso for feito sem esclarecimento aos impactados, eles foram vítimas de *shadow banning*. Nesse sentido, *shadow banning* consiste no uso de técnicas opacas de redução de

---

[39] SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press. 2017.
[40] *Ibidem*.

visibilidade de usuários ou publicações.[41, p. 2] Ele pode ocorrer, por exemplo, por meio da filtragem de conteúdo do *feed* de notícias (o conteúdo não chega a ser ranqueado), da atribuição de baixa relevância ao conteúdo, fazendo com que ele apareça no fim da lista de sugestões ou do *feed* de notícias, ou pela ausência de sugestão de autocompletar na busca por usuários, fazendo com que seja necessário digitar os valores exatos para obter sucesso na busca, e até mesmo pelo desaparecimento do usuário procurado no mecanismo de busca[42, p. 4].

No passado, o termo *shadow banning* era utilizado para designar a suspensão ou banimento do usuário sem o seu conhecimento, que seguia com acesso ao fórum e possibilidade de publicação, porém suas publicações não eram visíveis pelos outros usuários, mas apenas por ele mesmo. "Porque o usuário problemático não percebe o banimento, ele continua publicando para uma audiência fictícia ao invés de criar uma nova conta"[43, p. 1092].

Embora as plataformas neguem a prática de *shadow banning*, elas admitem a adoção de métodos reducionistas que se enquadram no que se entende por *shadow banning*. O YouTube, por exemplo, em 2019, informou que limitaria a recomendação de conteúdo que chegasse próximo de violar, porém não violasse, suas *Community Guidelines*, a fim de proporcionar melhor experiência aos usuários e balancear a liberdade de expressão com as responsabilidades da plataforma perante os usuários[44]. Nota-se que, nesse caso, é o YouTube que decide o que é conteúdo limítrofe passível de redução de visibilidade, ou seja, é uma entidade privada exercendo o controle sobre o exercício da liberdade de expressão com base na sua política interna. E para afastar dúvidas sobre a importância do sistema de recomendação do YouTube, a própria companhia revelou em 2018 que mais de 70%

---

[41] LEERSSEN, P. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. **Computer Law & Security Review**, v. 48, p. 1–13, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364923000018. Acesso em: 02/08/2023.

[42] LE MERRER, E.; MORGAN, B.; TRÉDAN, G. Setting the Record Straighter on Shadow Banning. **IEEE Conference on Computer Communications**. Disponível em: https://arxiv.org/abs/2012.05101. Acesso em: 10/08/2023

[43] SAVOLAINEN, Laura. The shadow banning controversy: perceived governance and algorithmic folklore. **Media, Culture & Society**, v. 44, n. 6, p. 1091-1109, 2022.

[44] Continuing our work to improve recommendations on YouTube. **YouTube Official Blog**, 2019. Disponível em: https://blog.youtube/news-and-events/continuing-our-work-to-improve/. Acesso em: 03/08/2023.

do conteúdo assistido em sua plataforma foi fruto de recomendação dos algoritmos[45].

Nos casos de *shadow banning*, não há notificação do usuário responsável pela publicação do conteúdo acerca da redução da visibilidade, fato que impossibilita o contraditório. O usuário não sabe se está acontecendo. E ainda que desconfie, não há nada que possa fazer a respeito, considerando que a prática é negada e de difícil prova. Além disso, não sabe o motivo da redução. Não há transparência no uso dessa técnica.

A redução de conteúdo, além de passar despercebida pelo usuário, é um mecanismo adotado pelas redes sociais para lidar com conteúdo problemático (limítrofe) sem exclui-lo[46, p. 6], já que a exclusão pode ser encarada como censura se não se basear na lei ou nos termos de serviço. A técnica também evita contestação, considerando a ausência de notificação do usuário. Por fim, a manutenção do conteúdo permite que usuários interessados o encontrem em busca ativa, ou eventualmente seguindo o autor da publicação, o que serve para o modelo de negócios adotado (circulação de usuários, obtenção de mais dados e venda de espaço publicitário), afinal, as manifestações, para as redes sociais, são apenas dados[47, p. 186].

O *shadow banning* e outras formas de governança das redes sociais e plataformas digitais afetam a liberdade de expressão ao filtrar, selecionar, ranquear, promover ou despromover o conteúdo entregue ou recomendado aos usuários, no cenário de digitalização da vida social. “[O] contexto atual da liberdade de expressão experimentou uma transformação problemática desde o ponto de vista constitucional, porque converte este direito em mero produto comercial, economicamente apreciável em função de seus resultados sem conexão alguma com a formação de uma opinião plural própria de um sistema democrático."[48, p. 187]

---

[45] SOLSMAN, J. E. YouTube's AI is the puppet master over most of what you watch. **CNET**, 2018. Disponível em: https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/. Acesso em: 03/08/2023.

[46] GILLESPIE, Tarleton. Do not recommend? Reduction as a form of content moderation. **Social Media+ Society**, v. 8, n. 3, julho-setembro, 2022. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/20563051221117552. Acesso em: 27/07/2023.

[47] CALLEJÓN, Francisco Balaguer. O impacto dos novos mediadores da era digital na liberdade de expressão. **Espaço Jurídico Journal of Law**, v. 23, n. 1, p. 179-204, 2022.

[48] *Ibidem*.

Por fim, e longe de esgotar os problemas relacionados à temática, "a redução também evita o escrutínio público, já que as intervenções são difíceis de detectar e não são – ainda – relatadas como parte das obrigações de transparência da plataforma"[49, p. 6]. É por isso que o debate público sobre o tema é de extrema relevância. A construção de caminhos para acomodar os direitos fundamentais em jogo deve envolver a sociedade, e não ficar restrita às plataformas.

Uma vez delineado o *shadow banning*, passa-se à investigação acerca da existência de regramento aplicável à técnica no Brasil, assim como do que se pode esperar do Congresso Nacional acerca do tema.

4 REGRAMENTO ATUAL E PERSPECTIVAS

A necessidade de harmonização entre os diversos direitos fundamentais de diferentes titulares em jogo nos faz recordar que não há direitos absolutos, e que a convivência das liberdades apenas é possível quando os seus limites são respeitados. Com a liberdade de expressão não deve ser diferente. A difusão da internet, em um primeiro momento, e o desenvolvimento de redes sociais, em um segundo, marcaram uma nova era para o exercício da liberdade de expressão, conferindo a todos com acesso à internet a possibilidade de manifestação do pensamento no ambiente virtual, assim como estabelecendo novos desafios para a manutenção desse novo espaço de convívio.

Há centenas de milhões de pessoas publicando em poucas redes sociais, o que faz com que cada uma dessas plataformas tenha enorme poder e responsabilidade. Poder para excluir organizar, filtrar, recomendar ou reduzir a divulgação das manifestações. Responsabilidade de empregar esforços para manter o ambiente inclusivo e livre de abusos, podendo, para tanto, excluir conteúdo ilegal, suspender e banir usuários. O grande alerta que se liga acerca do tema é que, nesses casos, o controle do exercício da liberdade de expressão se dá majoritariamente por entes privados, as redes sociais e plataformas digitais, por meio de mecanismos

[49] GILLESPIE, Tarleton. Do not recommend? Reduction as a form of content moderation. **Social Media+ Society**, v. 8, n. 3, julho-setembro, 2022. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/20563051221117552. Acesso em: 27/07/2023. Tradução livre.

internos desenvolvidos com base na autorregulação, com pouco ou nenhum regramento para balizar a legitimidade constitucional do ato.

No Brasil, por meio do Marco Civil da Internet, a liberdade de expressão foi destacada como fundamento[50] e princípio[51] da disciplina do uso de internet. Além disso, a Lei estabeleceu que é condição para o pleno exercício do direito de acesso à internet a garantia da liberdade de expressão na internet[52]. Apesar das referências mencionadas à liberdade de expressão, o Marco Civil da Internet pouco trata acerca da moderação de conteúdo pelas plataformas digitais, tangenciando o tema ao disciplinar a responsabilidade por danos decorrentes de conteúdo gerado por terceiros.

Sobre a retirada de conteúdo, a Lei estabelece que a plataforma deve tornar indisponível o conteúdo apontado por ordem judicial como infringente, sob pena de poder ser responsabilizada civilmente por conteúdo gerado por terceiros[53], devendo notificar o usuário responsável pelo conteúdo, conferindo-lhe informações que permitam o contraditório e a ampla defesa em juízo (ressalvados os casos de disposição de lei em contrário ou ordem judicial contrária e fundamentada)[54]. Ademais, o usuário responsável pode solicitar que a plataforma disponha, em substituição ao conteúdo tornado indisponível, a motivação ou a ordem judicial que deu fundamento à indisponibilização[55].

Percebe-se que a Lei não exige notificação do usuário acerca da exclusão de conteúdo com base em decisão da própria plataforma, nos casos de violação dos termos de serviço, o que torna o contraditório dispensável. A Lei tampouco dispõe sobre a recomendação algorítmica e sobre a redução de visibilidade de conteúdo. No Brasil não há exigência de transparência, e muito menos de fundamentação, em qualquer tipo de decisão tomada pelas redes sociais e plataformas digitais que

---

[50] BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.630, de 3 de julho de 2020.
5.568, de 14 de maio de 2013. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Art. 2º, *caput*. Disponível em:
https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334. Acesso em: 09/08/2023.
[51] *Idem.* Art. 3º, inciso I.
[52] *Idem.* Art. 8º, *caput*.
[53] *Idem.* Art. 19, *caput*.
[54] *Idem.* Art. 20, *caput*.
[55] *Idem.* Art. 20, parágrafo único.

envolva o direito fundamental à liberdade de expressão. Nesse sentido, o usuário sequer tem o direito de saber se suas publicações sofreram redução de visibilidade, ou o motivo para a redução. Sem o "se" e o "por que", resta inviabilizado o contraditório perante o ente privado, assim como quase impossibilitada a contestação do ato perante o poder judiciário.

O exercício da cidadania em meios digitais, outro dos fundamentos do Marco Civil da Internet[56], está longe de ser garantido enquanto não houver balizas para aferir a legitimidade constitucional do controle exercido pelos *gate keepers* da era digital sobre o exercício da liberdade de expressão.

Como possível solução para a problemática aqui debatida, o Projeto de Lei nº 2.630/2020, conhecido também por "PL das *fake news*", que pretende instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, em sua versão mais recente[57] até a elaboração deste artigo, tem como um dos objetivos estabelecer o direito do usuário à notificação, ao contraditório, à ampla defesa e ao devido processo em relação à moderação de conteúdos[58] realizada por redes sociais que tenham número médio mensal de usuários no Brasil superior a dez milhões[59]. O âmbito de proteção desse direito depende do que é considerada moderação de conteúdo: caso se entenda que apenas a exclusão de usuários e conteúdo seja moderação, têm-se um direito menos amplo; caso a redução e a ampliação de visibilidade de conteúdo também sejam considerados moderação, então visualiza-se um direito mais amplo. E foi a segunda opção a adotada[60] até então pelo Projeto de Lei.

De acordo com o Projeto de Lei, o usuário deverá ser notificado após as práticas de moderação de conteúdo, recebendo informações acerca da medida aplicada, a fundamentação da decisão com indicação das cláusulas dos termos de uso que sustentaram a medida, do procedimento e prazo para pedido de revisão da decisão, e dos critérios e procedimentos utilizados para a decisão[61]. O pedido de

---

[56] *Idem.* Art. 2º, inciso II.
[57] *Idem.*
[58] *Idem.* Art. 4, inciso III.
[59] *Idem.* Art. 2º, inciso I.
[60] *Idem.* Art. 5º, inciso V.
[61] *Idem.* Art. 18, inciso I.

revisão, a seu turno, deverá ser respondido em decisão fundamentada[62]. Além disso, os provedores deverão tornar pública toda ação de moderação de conteúdo[63].

Para assegurar maior transparência à moderação de conteúdo, os termos de uso deverão indicar os conteúdos proibidos, as etapas executadas para aferir a conformidade do conteúdo com os termos de uso, e informações sobre o mecanismo de contestação das decisões e sobre os critérios e métodos de moderação em contas e conteúdos[64]. Será ainda obrigatória a realização anual de auditoria externa independente, que, dentre outros aspectos, avaliará a ocorrência de discriminação ou de vieses nas decisões de moderação de contas e conteúdos[65].

A imposição legal de transparência quanto à moderação de conteúdo, em especial no que toca à quase invisível redução de visibilidade, significa avanço importante na proteção dos direitos fundamentais no âmbito das plataformas digitais, embora não esteja livre de críticas. Exigir transparência na moderação de conteúdo significa legitimar o grande poder moderador, obscurecendo outra questão: as plataformas deveriam ter todo esse poder[66, p. 5]? Sander sugere que o poder das plataformas deve ser regulado por variados ângulos, incluindo as regulações que tratam da proteção de dados, do direito eleitoral, da publicidade e do direito concorrencial, e destaca que "a proteção da liberdade de expressão online envolve necessariamente abordar as responsabilidades de uma gama muito mais ampla de atores que participam da esfera pública digital – incluindo, por exemplo, governos, partidos políticos, corretores de dados, organizações de mídia de massa, e anunciantes"[67, p. 1005-1006].

---

[62] *Idem.* Art. 18, inciso II.
[63] *Idem.* Art. 19, inciso I.
[64] *Idem.* Art. 20, incisos II, V, VII e VIII.
[65] *Idem.* Art. 24.
[66] MARONI, Marta. 'Mediated transparency': The Digital Services Act and the legitimisation of platform power. Publicado em abril de 2023. In LEINO-SANDBERG , Päivi; HILLEBRANDT, Maarten Zbigniew; KOIVISTO, Ida (editores). **(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice.** Editora Routledge. Livro ainda não publicado. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4413531. Acesso em: 31/07/2023.
[67] SANDER, B. Freedom Of Expression In The Age Of Online Platforms: The Promise And Pitfalls Of A Human Rights-Based Approach To Content Moderation. **Fordham International Law Journal**, v. 43, p. 939-1006, 2020. Disponível em: https://ir.lawnet.fordham.edu/ilj/vol43/iss4/3/. Acesso em: 11/08/2023.

CONSIDERAÇÕES FINAIS

Na sociedade hiperconectada, que é causa e consequência do mencionado capitalismo de plataforma de Srnicek, as redes sociais, plataformas que fazem a intermediação de pessoas e de conteúdo gerado por milhões ou bilhões de usuários, adquiriram poderes para influenciar o que é mais ou menos consumido em termos de conteúdo. Tais poderes são exteriorizados por meio da moderação de conteúdo, realizada com base na obtenção e processamento massivo de dados dos usuários, no caso de recomendação e disponibilização de conteúdo, ou com base nos termos de serviços, nos casos de exclusão de conteúdo e de suspensão e banimento de usuários. Esse cenário evidencia o papel decisivo das redes sociais sobre no exercício da liberdade de expressão e a necessidade de investigação sobre a suficiência da regulamentação da moderação de conteúdo.

O que se pode perceber a partir da análise legislativa é que a moderação de conteúdo não foi objeto de regulamentação no ordenamento jurídico brasileiro. Isso significa que as redes sociais não têm dever de transparência, e que o poder público não tem diretrizes para aferir a legitimidade constitucional da prática. Não só a redução e exclusão de conteúdo e a suspensão e o banimento de usuários devem debatidos publicamente e em âmbito legislativo, mas também a ampliação de visibilidade (de *fake news*, por exemplo).

Quanto ao *shadow banning*, o cenário atual é igualmente preocupante. Primeiro, o usuário dificilmente terá condições de saber se ele ou suas publicações foram objeto de redução de visibilidade. Segundo, não há obrigatoriedade de notificação do usuário por parte das redes sociais acerca da redução. Terceiro, não há obrigatoriedade de fundamentação da decisão. Quarto, não há direito ao contraditório. Quinto, os itens anteriores prejudicam o exercício do contraditório em juízo.

A esperança mais concreta de avanço na defesa da liberdade de expressão em âmbito digital está depositada atualmente no Projeto de Lei nº 2.630/2020, que, inspirado no *Digital Services Act da União Europeia*, busca, dentre outros objetivos, implementar uma série de regras para a moderação de conteúdo pelas redes sociais cujo número médio mensal de usuários no Brasil supere dez milhões.

Este texto objetivou destacar alguns dos desafios que surgiram a partir do avanço da tecnologia da informação e da comunicação, com o intuito de contribuir para a harmonização da tecnologia com o respeito à liberdade de expressão. A posição monopolística e a situação de poder em que se colocaram algumas *big techs* titulares de redes sociais é fruto do sucesso de seu modelo de negócios. Portanto, não se pode esquecer que se trata de empresas privadas que buscam lucros, e não há nada errado nisso, devendo os Estados estimular conversas sobre o tema e eventualmente discutir a possibilidade de elaboração de tratado internacional para proteger direitos humanos no uso de redes sociais. Por fim, no capitalismo de vigilância, a educação digital é outro caminho possível para a defesa dos direitos fundamentais.

REFERÊNCIAS BIBLIOGRÁFICAS

BRANCO, Dácio Castelo. 7 em cada 10 brasileiros se informa por redes sociais — e isso afeta a segurança. **Canaltech**, 2021. Disponível em: https://canaltech.com.br/seguranca/7-em-cada-10-brasileiros-se-informa-por-redes-sociais-e-isso-afeta-a-seguranca-198668/. Acesso em: 12/05/2023.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 2.630, de 3 de julho de 2020. 5.568, de 14 de maio de 2013. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334. Acesso em: 09/08/2023.

BUSTAMANTE, Javier. Poder comunicativo, ecossistemas digitais e cidadania digital. In: SILVEIRA, Sergio Amadeu da. **Cidadania e Redes Digitais**. São Paulo: Maracá – Educação e Tecnologias, 2010.

CALLEJÓN, Francisco Balaguer. O impacto dos novos mediadores da era digital na liberdade de expressão. **Espaço Jurídico Journal of Law**, v. 23, n. 1, p. 179-204, 2022.

CHAFFEY, Dave. What happens online in 60 seconds in 2021? **Smart Insights**, 2021. Disponível em: https://www.smartinsights.com/internet-marketing-statistics/happens-online-60-seconds/. Acesso em: 26/07/2023.

CHAFFEY, Dave. Global social media statistics research summary 2023. **Smart Insights**, 2023. Disponível em: https://www.smartinsights.com/social-media-

marketing/social-media-strategy/new-global-social-media-research/. Acesso em: 26/07/2023.

Continuing our work to improve recommendations on YouTube. **YouTube Official Blog**, 2019. Disponível em: https://blog.youtube/news-and-events/continuing-our-work-to-improve/. Acesso em: 03/08/2023.

CUOFANO, Gennaro. How Much Money does Google make from advertising? **FourWeekMBA**, 2023. Disponível em: https://fourweekmba.com/how-much-money-does-google-make-from-advertising/. Acesso em: 28/07/2023.

DE LUCA, Aldo. Pesquisa do Instituto Reuters em 46 países confirma poder das mídias sociais como fonte de notícias. **Media Talks**, 2023. Disponível em: https://mediatalks.uol.com.br/2023/06/14/pesquisa-mostra-poder-das-midias-sociais-para-acesso-a-noticias-no-mundo/. Acesso em: 24/07/2023.

FODERARO, Lisa W. Taking a Call for Climate Change to the Streets. **The New York Times**, 2014. Disponível em: https://www.nytimes.com/2014/09/22/nyregion/new-york-city-climate-change-march.html. Acesso em: 25/07/2023.

FREDES, Andrei Ferreira. Liberdade de expressão e configuração do ambiente virtual: o controle do fluxo de informação e expressão na internet. In: SARLET, Ingo Wolfgang; RUARO, Regina Linden; LEAL, Augusto Antônio Fontanive (orgs.). **Direito, Ambiente e Tecnologia: estudos em homenagem ao professor Carlos Alberto Molinaro**. Porto Alegre: Fundação Fênix, 2021. p. 401-423.

GILLESPIE, Tarleton. Do not recommend? Reduction as a form of content moderation. **Social Media+ Society**, v. 8, n. 3, julho-setembro, 2022. Disponível em: https://journals.sagepub.com/doi/epub/10.1177/20563051221117552. Acesso em: 27/07/2023.

Hours of video uploaded to YouTube every minute as of February 2022. **Statista**, 2023. Disponível em: https://www.statista.com/statistics/259477/hours-of-video-uploaded-to-youtube-every-minute/. Acesso em: 26/07/2023.

LE MERRER, E.; MORGAN, B.; TRÉDAN, G. Setting the Record Straighter on Shadow Banning. **IEEE Conference on Computer Communications**, 2021. Disponível em: https://arxiv.org/abs/2012.05101. Acesso em: 10/08/2023

LEISER, M. R. Analysing the European Union's Digital Services Act Provisions for the Curtailment of Fake News, Disinformation, & Online Manipulation. Data da publicação: maio de 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4427493. Acesso em: 01/08/2023.

LEERSSEN, P. An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. **Computer Law & Security**

Review, v. 48, p. 1–13, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364923000018. Acesso em: 02/08/2023.

MARONI, Marta. 'Mediated transparency': The Digital Services Act and the legitimisation of platform power. Publicado em abril de 2023. In LEINO-SANDBERG , Päivi; HILLEBRANDT, Maarten Zbigniew; KOIVISTO, Ida (editores). **(In)visible European Government: Critical Approaches to Transparency as an Ideal and a Practice.** Editora Routledge. Livro ainda não publicado. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4413531. Acesso em: 31/07/2023.

SANDER, B. Freedom Of Expression In The Age Of Online Platforms: The Promise And Pitfalls Of A Human Rights-Based Approach To Content Moderation. **Fordham International Law Journal**, v. 43, p. 939-1006, 2020. Disponível em: https://ir.lawnet.fordham.edu/ilj/vol43/iss4/3/. Acesso em: 11/08/2023.

SARLET, Ingo Wolfgang; HARTMANN, Ivar. Direitos fundamentais e direito privado: a proteção da liberdade de expressão nas mídias sociais. **RDU**, Porto Alegre, Volume 16, n. 90, p. 85-108, 2019.

SAVOLAINEN, Laura. The shadow banning controversy: perceived governance and algorithmic folklore. **Media, Culture & Society**, v. 44, n. 6, p. 1091-1109, 2022.

SOLSMAN, J. E. YouTube's AI is the puppet master over most of what you watch. **CNET**, 2018. Disponível em: https://www.cnet.com/tech/services-and-software/youtube-ces-2018-neal-mohan/. Acesso em: 03/08/2023.

SRNICEK, Nick. **Platform capitalism**. Cambridge: Polity Press. 2017.

UNIAO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral Sobre a Proteção de Dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 02/08/2023.

VOLOKH, Eugene. Cheap speech and what it will do. **Yale LJ**, v. 104, p. 1805-1850, 1994.

WEST, Sarah Myers. Data capitalism: Redefining the logics of surveillance and privacy. **Business & society**, v. 58, n. 1, p. 20-41, 2019.

YORK, Jillian C.; ZUCKERMAN, Ethan. Moderating the public sphere. In Jørgensen, R. F. (Ed.), **Human rights in the age of platforms**, v. 137, p. 137-161, 2019.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. Journal of information technology, v

4. INTELIGÊNCIA ARTIFICIAL E RESPONSABILIDADE CIVIL: UMA ANÁLISE DOS MECANISMOS DE RESPONSABILIZAÇÃO NO BRASIL

ARTIFICIAL INTELLIGENCE AND CIVIL LIABILITY: AN ANALYSIS OF ACCOUNTABILITY MECHANISMS IN BRAZIL

https://doi.org/10.36592/9786554600712-04

Helen Lentz Ribeiro Bernasiuk[1]

SUMÁRIO

PRIMEIRA PARTE: 1. Inteligência Artificial: Breve Fundamentação Teórica; 2. Algumas aplicações no uso de IA; 3. Personalidade jurídica dos robôs. SEGUNDA PARTE: 1. Responsabilidade Civil de IA na União Europeia; 2. Responsabilidade Civil de IA no BR (PL Projeto de Lei n. 2338, de 2023); 3. (Des) necessidade de regulamentação específica acerca da Responsabilidade Civil de IA no Direito brasileiro?; Conclusão. Referências.

RESUMO

O presente artigo tem como objetivo analisar as imbricações entre inteligência artificial e responsabilidade civil, na perspectiva do direito brasileiro. A justificativa da pesquisa se dá, porquanto na Sociedade da Informação/ Digital, a utilização de sistemas de inteligência artificial já é uma realidade e podem gerar diversos danos. Nesse aspecto, será analisada a discussão no âmbito da União Europeia, bem como no Projeto de Lei nº 2338, de 2023, acerca da temática no Brasil. Ainda, se os mecanismos já existentes na sistemática brasileira são suficientes para resolução de conflitos envolvendo a temática. O método exploratório, sob o viés qualitativo, apresenta-se como via para subsidiar reflexões e conclusões, ainda que provisórias, sobre responsabilidade civil e IA Procede-se, neste recorte de estudo, às técnicas de pesquisa bibliográfica e documental, pelas quais se buscam leis, normativas e orientações sobre o tema. A interpretação dos dados se dá via método sociológico. Ressalta-se que o presente artigo integra a linha de pesquisa *Direito, Ciência,*

---

[1] Doutoranda em Direito pela PUCRS. Mestre em Direito pela PUCRS. Especialista em Direito Civil pela UFRGS. Especialista em Direito Público pela Uniderp. Diritto Costituzionale Comparato e Cultura Giuridica Europea pela Sapienza, Università di Roma (Roma- Itália). La constitución del algoritmo:Inteligencia artificial y Derecho, Universidad de Granada (Granada- Espanha). Bolsista Capes/Proex PPGD/PUCRS. Currículo Lattes: http://lattes.cnpq.br/4798723812833494. Orcid: https://orcid.org/0000-0002-6224-1251. Advogada.
E-mail: helenbernasiuk@gmail.com.

Tecnologia & Inovação, do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).
Palavras-chave: Inteligência artificial- Responsabilidade Civil- Sociedade Digital.

ABSTRACT

This article aims to analyze the overlap between artificial intelligence and civil liability, from the perspective of Brazilian law. The justification for the research is that in the Information/Digital Society, the use of artificial intelligence systems is already a reality and can cause various damages. In this aspect, the discussion will be analyzed within the scope of the European Union, as well as in Bill No. 2338, of 2023, on the topic in Brazil. Furthermore, whether the mechanisms already existing in the Brazilian system are sufficient to resolve conflicts involving the issue. The exploratory method, under a qualitative bias, presents itself as a way to support reflections and conclusions, even if provisional, on civil liability and AI. In this study section, bibliographic and documentary research techniques are sought, through which we seek laws, regulations and guidelines on the subject. Data interpretation takes place via sociological method. It should be noted that this article is part of the Law, Science, Technology & Innovation research line of the Postgraduate Program in Law at the Pontifical Catholic University of Rio Grande do Sul (PUCRS).
Keywords: Artificial intelligence- Civil Responsibility- Digital Society.

INTRODUÇÃO

A temática envolvendo responsabilidade civil e inteligência artificial tem gerado inúmeras discussões, tanto a nível nacional como a nível internacional. É inegável os benefícios de utilização desses sistemas, mas sua aplicação a depender do contexto pode criar riscos excessivos para usuários e desenvolvedores. Nesse aspecto, o objetivo desse *paper,* na primeira parte, é tecer breves considerações acerca do conceito de IA, analisar algumas de suas aplicações, a fim de demonstrar a sua ampla utilização, nas mais diversas searas. Será, ainda, abordada a questão da personalidade jurídica dos robôs. Na segunda parte, abordaremos alguns pontos acerca da responsabilidade civil no âmbito da União Europeia e como está sendo tratado nos Projeto de Lei acerca da temática no Brasil. Por fim, a partir da regulamentação já existente no direito brasileiro, verificaremos se há necessidade de uma lei específica sobre a temática ou se o que consta no nosso sistema jurídico é suficiente para a solucionar questões atinentes à responsabilidade civil. Importante salientar a necessidade de observância de padrões éticos como pressuposto para utilização desses sistemas.

1 Inteligência Artificial: Breve Fundamentação Teórica

A Inteligência Artificial (doravante IA)[2] é uma das tecnologias mais disruptivas e relevantes do século XXI,[3]sendo utilizada em larga escala no cotidiano. Um caso que exemplifica o exposto é a ferramenta ChatGPT, da empresa OpenAI, a qual teve uma divulgação mundial e vem sendo utilizada nos diversos segmentos.

Para que seja considerada uma IA "é preciso que essa máquina imite nossa atividade mental quando estamos fazendo uma operação aritmética," ou seja, não basta apenas "projetar e criar uma máquina de calcular".[4] Nesse aspecto, de forma simplificada, importante conceituar o algoritmo como "uma sequência finita de passos que se usa para resolver um problema"[5].

A proposta de legislação acerca da temática no Parlamento Europeu entende como inteligência artificial "uma família de tecnologias em rápida evolução, capaz de oferecer um vasto conjunto de benefícios económicos e sociais a todo o leque de indústrias e atividades sociais".[6] Os conceitos de IA podem modificar a depender da abordagem a ser utilizada.[7]"

---

[2] TURING, Alan. **Discussion on the mind and the computing machine**. 27.out.1949. Disponível em: http://www.turing.org.uk/sources/wmays1.html. Acesso em: 10 abr.2023.

[3] COMISSÃO EUROPEIA. Grupo Europeu de Ética na Ciência e Novas Tecnologias. **Declaração de Inteligência Artificial, Robótica e Sistemas 'Autônomos'**. Bruxelas, 9 de março de 2018. Disponível em: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. Acesso em: 8 fev. 2023.

[4] TEIXEIRA, João de Fernandes. **O que é inteligência artificial** (recurso eletrônico). Porto Alegre, RS: Editora Fi, 2017, p. 16.

[5] BRIAN, Christian; GRIFFITHS, Tom. **Algoritmos para viver***:* a ciência exata das decisões humanas. São Paulo: Companhia das Letras, 2017, que se estendem sobre o que são algoritmos às p. 13,14 e 16.

[6] UNIÃO EUROPEIA, PARLAMENTO EUROPEU. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2022, Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 09 abr.2023.

[7] Consoante exemplificado na tese de doutorado do Juiz Federal Erick Navarro, exemplifica os diferentes tipos de Inteligência Artificial, porquanto algumas se assemelham ao pensamento humano, denominadas "reasonig"; semelhanças comportamentais, chamadas "behavior" e, também, podem ser analisadas pela acurácia das decisões geradas pelo sistema, quando são denominadas de "rationality". IN: WOLKART, Erick Navarro. **Análise econômica e comportamental do processo civil: como promover a cooperação para enfrentar a tragédia da Justiça no processo civil brasileiro**. 2018. 815 f. Tese (Doutorado) – Programa de Pós-graduação em Direito, Universidade do Estado do Rio de Janeiro – UERJ, Rio de Janeiro, 2018. p. 664. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/17363. Acesso em: 07 fev. 2023.

No Brasil, a Estratégia Brasileira de Inteligência Artificial (EBIA), possui como objetivo traçar um plano de desenvolvimento de estratégias acerca de Inteligência Artificial, bem como alinhar a necessidade de uma abordagem ética para a utilização de tais sistemas.[8]

Uma das dificuldades se refere à conceituação do que seria inteligência artificial. Nesse aspecto, a comissão de juristas instituídas pelo Ato do Presidente do Senado nº 4, de 2022[9], destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos projetos brasileiros acerca da temática não conseguiu chegar a uma conclusão unânime do conceito de IA.

Essa minuta de substitutivo originou o Projeto de Lei nº 2338, de 2023, que, por fim, define IA como sendo o "sistema computacional, com graus diferentes de autonomia, desenhado para inferir como atingir um dado conjunto de objetivos", os quais, utilizando abordagens baseadas em aprendizagem de máquina e/ou lógica e representação do conhecimento, por meio de dados de entrada provenientes de máquinas ou humanos, com o objetivo de produzir previsões, recomendações ou decisões que possam influenciar o ambiente virtual ou real".[10]

Cumpre salientar que a utilização de um protocolo ético é pressuposto para utilização de IA, como, o respeito à diversidade e à privacidade; a dignidade da vida, a indelegabilidade da decisão que seja intrinsicamente humana; a necessidade de uma segurança preventiva e precavida; a necessidade de supervisão humana e reversibilidade, dentre outros[11].

---

[8] Instituída pela Portaria MCTI nº 4.617, de 6 de abril de 2021, alterada pela Portaria MCTI nº 4.979, de 13 de julho de 2021 (Anexo). BRASIL, Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial – EBIA.** Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Acesso em: 05 abr. 2023.

[9] BRASIL, SENADO FEDERAL. RELATÓRIO FINAL Comissão de Juristas instituída pelo Ato do Presidente do Senado nº 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relato%CC%81rio%20final%20CJSUBIA.pdf. Acesso em: 02 abril 2023, p. 80.

[10] Conforme se verifica do art. 4º. BRASIL, Senado Federal. Projeto de Lei nº 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1683629462652&disposition=inline&_gl=1*cmo644*_ga*MTQ3NTM0NjAzNS4xNjQ1NTc1MDc1*_ga_CW3ZH25XMK*MTY4MzY3MjcyMS4zLjAuMTY4MzY3MjcyMy4wLjAuMA. Acesso em: 09 maio 2023.

[11] FREITAS, Juarez. **Direito e inteligência artificial**: em defesa do humano. Belo Horizonte: Fórum, 2020. p.74.

Alguns parâmetros devem ser observados quando se utiliza IA, como a autonomia humana; prevenção de danos; equidade e explicabilidade[12]. Importante salientar das situações em que não é possível a explicabilidade, ocasião em que deve ser utilizadas medidas como rastreabilidade, a auditabilidade e a comunicação transparente sobre as capacidades do sistema, desde que o sistema, no seu conjunto, respeite os à observância dos direitos fundamentais.[13]

Há a necessidade de se observar o desenvolvimento ético da inteligência artificial desde a concepção do sistema.[14] No âmbito do Poder Judiciário Brasileiro, o Conselho Nacional de Justiça, dispõe na Resolução nº332[15] o respeito aos direitos fundamentais.[16] como requisito para utilização desses sistemas pela justiça. Assim, no próximo item será abordada algumas aplicações no uso de IA.

---

[12] O conteúdo do documento é de responsabilidade do grupo de peritos de alto nível sobre a inteligência artificial (GPAN IA). As posições não podem ser consideradas como posição oficial da Comissão Europeia. COMISSÃO EUROPEIA. **Orientações éticas para uma IA de confiança**: Bruxelas: Comissão Europeia, 2019. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF. Acesso em: 05 maio 2023.

[13] COMISSÃO EUROPEIA. **Orientações éticas para uma IA de confiança**: Bruxelas: Comissão Europeia, 2019. Disponível em: https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-pt/format-PDF. Acesso em: 05 maio 2023.

[14] RUARO, Regina Linden; REIS, Ludmila Camilo Catão Guimarães. Los retos del desarrollo ético de la Inteligencia Artificial. **Veritas**, v. 65, n. 3, set.-dez. 2020, p. 1-14, p. 05. http://dx.doi.org/10.15448/1984-6746.2020.3.38564. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8086046. Acesso em: 09 maio 2023.

[15] BRASIL, Conselho Nacional de Justiça. **Resolução nº332, de 21 de agosto de 2020**. **Dispõe sobre a ética, transparência e a governança na produção e no uso da Inteligência Artificial no Poder Judiciário e dá outras providências**. Disponível em:https://www.cnj.jus.br/wp-content/uploads/2020/08/Resolu%C3%A7%C3%A3o-332-IA-Programa%C3%A7%C3%A3o_v4-.pdf. Acesso em: 25 mar. 2023.

[16] A dificuldade de conceituar *Direitos Fundamentais* se dá pelas diversas expressões usadas para designá-los (direitos naturais, humanos, do homem, individuais e direitos públicos subjetivos, bem como liberdades fundamentais e públicas) In: SILVA, José Afonso da Silva. **Curso de Direito Constitucional Positivo**. 36. ed. rev. e atual. São Paulo: Malheiros, 2013. p. 177. Conforme assinala o professor Ingo Sarlet há diferenças entre as expressões direitos humanos e fundamentais. Desse modo, os direitos humanos são os constantes em documentos internacionais, que almejam a validade universal para todos os povos, e possuem um caráter internacional. Os direitos fundamentais são direitos positivados no âmbito do direito constitucional de determinado Estado. In: SARLET, Ingo Wolfgang. **A eficácia dos Direitos Fundamentais**. 12. ed. Porto Alegre: Livraria do Advogado, 2015. p. 29.

2 Algumas aplicações no uso de IA

A utilização de IA já vem sendo utilizada em diversas searas, como nos cuidados de saúde, na agricultura, na educação, na gestão das infraestruturas, na energia, nos transportes e logística, nos serviços públicos, na segurança, na justiça, na administração pública, em sistemas de justiça, dentre outros.

O Poder Judiciário Brasileiro, em 2022, apontou um expressivo aumento de projetos de inteligência artificial. No âmbito do "Projeto Judiciário 4.0" [17], apresentado pelo ministro Luiz Fux, foram identificados 111 projetos desenvolvidos ou em desenvolvimento nos tribunais. O Supremo Tribunal Federal já possui três IA's em funcionamento: Victor, [18] "RAFA"[19] e da "Vitória"[20].

A Administração Pública também já utiliza diversos sistemas de IA'S, o Tribunal de Contas da União, por exemplo, utiliza a "Alice", que auxilia na análise de licitações e editais; a "Sofia", que auxilia os auditores e a "Monica", que auxilia no monitoramento Integrado para o controle de aquisições. Tais ferramentas auxiliam

---

[17]O número de iniciativas cresceu em torno de 171% em relação ao levantamento realizado em 2021, quando haviam sido informados apenas 41 projetos. Também ocorreu o aumento de projetos de IA que desenvolvem soluções desses sistemas. BRASIL, Conselho Nacional de Justiça, 2022**. Justiça 4.0: Inteligência artificial está presente na maioria dos tribunais brasileiros**. Disponível em: https://www.cnj.jus.br/justica-4-0-inteligencia-artificial-esta-presente-na-maioria-dos-tribunais-brasileiros/. Acesso em: 18 março 2023.

[18] Acerca do projeto "Victor", para uma análise de forma aprofundada vide: IN: BERNASIUK, Helen Lentz Ribeiro. A inteligência artificial e a necessidade de observância de princípios fundamentais: Victor no Supremo Tribunal Federal. p. 169-19. In: CALIENDO, Paulo; ALFF, Hannah Pereira (Orgs.). **Temas atuais de processo tributário**. Porto Alegre: Editora Fundação Fênix, 2022. 437 p. Disponível em: https://www.fundarfenix.com.br/_files/ugd/9b34d5_e856932e6d1a4c4cb8ee2da47a016f06.pdf . Acesso em 27 mar. 2023.

[19] A RAFA 2030 (Redes Artificiais Focadas na Agenda 2030) "é uma ferramenta de inteligência artificial lançada em 2022 para apoiar a classificação de acórdãos ou de petições iniciais em processos do STF na Corte de acordo com os ODS, por meio de comparação semântica". BRASIL, Supremo Tribunal Federal. Disponível em:
https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=505767&ori=1#:~:text=A%20RAFA%202030%20(Redes%20Artificiais,por%20meio%20de%20compara%C3%A7%C3%A3o%20sem%C3%A2ntica. Acesso em: 19 maio 2023.

[20] BRASIL, Supremo Tribunal Federal. Ministra Rosa Weber lança robô VitórIA para agrupamento e classificação de processos: a nova ferramenta dará mais celeridade ao andamento processual e resultará em mais segurança jurídica. Disponível em:
https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=507426&ori=1. Acesso em 19 maio 2023.

na análise de editais de licitação, de relatórios internos e diversos comandos auxiliando a gestão pública.[21]

Na Europa, para alguns crimes, há o sistema "predicitive policing", o qual utiliza IA para prevenir delitos. Nesse caso, além de ser reativa, se torna também preditiva e preventiva. Assim, "la capacità preditiva dell'algoritmo è funzionalmente orientata alla prevenzione, consentendo alle forze di sicurezza di anticipare la loro risposta." Na Itália, chama-se "Key- Crime" e, na Espanha, Veri Pol e Vio Gén. [22]

Na China, já foi lançada a primeira âncora virtual de telejornal, criada por Inteligência Artificial. A robô, chamada "Ren Xiaorong" reúne as carcatéristicas de mil apresentadores, o que auxiliou na formação de suas habilidades, bem como se mantém no ar 24 horas por dia, nos 365 dias do ano.[23]

Quanto aos carros autônomos, governos de diversos países estão discutindo regulações acerca da responsabilidade por acidentes. Carros autônomos atropelarem e provocarem a morte já não é mais utopia[24]. O Reino Unido[25], por exemplo, pretende responsabilizar montadoras por acidentes em carros autônomos.

O robô "Xiaoby" passou no exame para o exercício da medicina, o denominado " National Medical Licensing Examination" na China. O objetivo é o de servir de apoio aos profissionais, revisando histórico clínico do paciente e sugerir um tratamento.[26]

---

[21] FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. **Arbitrium ex machina***:* panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**. Vol. 995, p. 635 – 655 (Set / 2018), p. 636/637.

[22] De ressaltar que a utilização é excepcional, para crimes específicos, crimes de rua, cometidos em série, como furtos e roubos. Ainda, a tradução livre: "a capacidade preditiva do algoritmo está funcionalmente orientada para a prevenção, permitindo às forças de segurança antecipar a sua resposta". FAGGIANI, Valentina. La lotta contro il crimine attraverso gli algoritmi: contraddizioni e profili di (in) constituzionalitá dell' applicazione dell' IA ala giustizia penale. CARRILLO, Francisco Javier Garrido; FAGGIANI, Valentina (coord.). **Respuesta Institucional y normativa al crime organizado**: Perfiles estratégicos para uma lucha eficaz. Minesota: Thomson Reuters, 2022, p. 245- 281. p. 254.

[23] VENTURA, Duda. **China lança primeira âncora virtual de telejornal, criada por Inteligência Artificial**. Disponível em:https://istoe.com.br/o-avatar-da-noticia/. Acesso em:15 abr. 2023.

[24] FREIRE, Raquel. **Carro autônomo da Uber atropela e mata mulher nos EUA: Empresa suspendeu todos os testes com carros autônomos na América do Norte.**19/03/2018. Disponível em: https://autoesporte.globo.com/videos/noticia/2018/03/carro-autonomo-da-uber-atropela-e-mata-mulher-nos-eua.ghtml. Acesso em: 16 abr. 2023.

[25] CNN BRASIL, Economia. **Reino Unido quer responsabilizar montador por acidentes de carros autônomos**. Disponível em: https://www.cnnbrasil.com.br/economia/reino-unido-quer-responsabilizar-montadoras-por-acidentes-de-carros-autonomos/amp/. Acesso em: 16 abr.2023.

[26] GIL MEMBRADO, Cristina. **Una nueva era: hacia el robot sanitario autónomo y su encaje en el derecho.** U p. 357-399, 2022, p. 370.

Na área da medicina, a IA já vem sendo utilizada em grande escala, como por exemplo, em cirurgias robóticas[27]. Ainda, é capaz de auxiliar em diagnósticos médicos, prevendo a incidência de câncer de mama[28], com cinco anos de antecedência de sua manifestação.

A IA generativa, como é o ChatGPT podem atuar em diversas demandas, inclusive auxiliando diagnósticos médicos[29]. A telemedicina é um setor que deve movimentar mais de U$ 130 bilhões até 2025 e a tendência é de aumento contínuo por demandas de pacientes nessa modalidade, incentivo a médicos e operadoras de saúde, bem como uma escalada de implementação de sistemas de inteligência artificial[30].

Desse modo, inúmeras são as aplicações de IA, em diversas segmentos da sociedade, razão pela qual a importância do debate acerca da responsabilidade civil por danos causos por esses sistemas.

3 Personalidade jurídica dos robôs.

A medida em que a IA torna-se cada vez mais autônoma, indaga-se acerca de seu funcionamento e, a partir daí, surge o questionamento de quem seria responsável pelos danos por ela causados.[31] Nesse aspecto, poderia ser o fabricante, o desenvolvedor ou aquele que a utiliza para as suas atividades profissionais. Assim,

---

[27] Cirurgia robótica é o "tratamento cirúrgico a ser realizada por via minimamente invasiva, aberta ou combinada, para o tratamento de doenças em que já se tenha comprovado sua eficácia e segurança Conforme se verifica do art. 1º da Resolução nº 2311/2022. CONSELHO FEDERAL DE MEDICINA. **Resolução nº 2311/2022**. Regulamenta a cirurgia robótica no Brasil. Brasília: CFM, 2022. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2022/2311. Acesso em: 31 março 2023.

[28] BRASIL, Sociedade Brasileira de Mastologia. **Inteligência Artificial prevê câncer de mama cinco anos antes**. Disponível em: https://www.sbmastologia.com.br/inteligencia-artificial-preve-cancer-de-mama-cinco-anos-antes/. Acesso em: 31 março 2023.

[29] MONTERASTELLI, Alessandra. Enfermeiros robôs, inteligência artificial e os interesses da maioria. Entrevista concedida a Cátia Rizzatti. **Instituto Humanitas Unisinos**, 21 jan. 2022. Disponível em: https://www.ihu.unisinos.br/626135-enfermeiros-robos-inteligencia-artificial-e-os-interesses-da-maioria-entrevista-especial-com-alessandra-monterastelli. Acesso em: 04 maio 2023.

[30] CABRINI, Natália. 6 Tendências da Telemedicina no Brasil em 2022. **Medicina S/A**, [*s.l.*], 03 mai. 2022. Disponível em: https://medicinasa.com.br/6-tendencias-telemedicina/. Acesso em: 15 jun. 2023.

[31] DE ANDRADE, Fabio Siebeneichler; FACCIO, Lucas Girardello. Notas sobre a responsabilidade civil pela utilização da inteligência artificial. **DOUTRINA NACIONAL**, v. 46, n. 146, p. 153 e ss., 2019.

iniciaram-se discussões acerca da personalidade jurídica dos robôs (pessoa eletrônica).

A personalidade jurídica dos robôs foi abordada pela primeira vez por Lawrence B. Solum, em 1992 e o cerne da discussão era a possibilidade de os robôs agirem de forma racional.[32]

No ano de 2017 é concedida a cidadania árabe para um robô com inteligência artificial, intitulada de "Sofia". Ela possuía mais de 60 expressões faciais para manter a conversação e interagir e material que emula a pele humana.[33]

O Parlamento Europeu, por exemplo, fez recomendações sobre regras de Direito Civil e Robótica no início de 2017, chamando atenção para a necessidade de regular o desenvolvimento dos robôs autônomos e inteligentes. Outra recomendação é antever a possibilidade de uma personalidade jurídica para eles[34].

Na Resolução do Parlamento Europeu, uma das questões aventadas, em 2017, foi a regulação de sistemas autônomos de IA. O órgão, em suas considerações iniciais, levando em consideração o estado avançado da robótica e da IA, discorre sobre alguns dos potenciais problemas que poderão surgir para a responsabilidade civil em razão do desenvolvimento desses sistemas:

> Considerando que, graças aos impressionantes avanços tecnológicos da última década, não só os robôs de hoje conseguem efetuar atividades que, regra geral, costumavam ser exclusivamente realizadas por humanos, como também o desenvolvimento de certas características autónomas e cognitivas – por exemplo, a capacidade de aprender com a experiência e de tomar decisões quase independentes – os tornaram cada vez mais similares a agentes que interagem com o seu ambiente e conseguem alterá-lo de forma significativa; considerando

---

[32] SOLUM, Lawrence B. Legal Personhood for Artificial Intelligences. North Carolina Law Review, vol. 70,1192, p. 1321ss.

[33] PAULO, Guilherme. Sophia é a primeira robô da história a ter cidadania oficial em um país. 26/10/2017. Disponível em: https://www.tecmundo.com.br/produto/123533-sophia-primeira-robo-historia-ter-cidadania-oficial-pais.htm. Acesso em: 1º julho 2023.

[34] PARALAMENTO EUROPEU. UNIÃO EUROPEIA. **Resolução do Parlamento Europeu de 16 de fevereiro de 2017**, com recomendações à Comissão de Direito Civil sobre Robótica. Disponível em: https://solene-gerardin.com/16-february-2017-european-parliament-resolution-with-recommendations-to-the-commission-on-civil-law-rules-on-robotics/. Acesso em: 26 março 2023.

que, nesse contexto, a responsabilidade jurídica decorrente de uma ação lesiva de um robô constitui uma questão crucial.[35]

O referido documento faz menção a problemas que podem advir quanto à aplicação de normas já existentes, porquanto os sistemas de IA podem demonstrar situações imprevisíveis. Esses sistemas utilizam processos de aprendizado, e não necessariamente cognitivos humanos, razão pela qual, muitas vezes, sequer desenvolvedores/ programadores terão conhecimento de determinada tarefa por ele realizadas. [36].

No âmbito do Direito, destaca-se uma tese de doutorado que versa sobre novo paradigma acerca da personalização da IA. O pesquisador entende que o direito deve personalizar entes não humanos de IA de acordo com suas capacidades cognitivas[37].

A questão da personalidade jurídica do robô se encontra superada, porquanto em 20 de outubro de 2020, foi aprovada nova Resolução do Parlamento Europeu, contendo recomendações à Comissão sobre o regime de responsabilidade civil aplicado à IA (2020/2014- INL)[38]. Nesse aspecto, cumpre transcrever o trecho

---

[35] Conforme se verifica do item "z" do Regulamento que trata acerca da responsabilidade. UNIÃO EUROPEIA. Parlamento Europeu. **Resolução do Parlamento Europeu, de 16 de fevereiro de 2017, que contém recomendações à Comissão sobre disposições de Direito Civil sobre Robótica**. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_PT.html. Acesso em: 28 março 2023.

[36] À título exemplificativo, cita-se um caso emblemático, em que o Facebook criou dois robôs para negociar produtos com seres humanos e com outras máquinas. No caso em questão, foi criada uma versão simplificada da linguagem, que utilizava as palavras de forma a evidenciar apenas os aspectos relevantes da negociação. Embora essa nova linguagem não fizesse sentido aos desenvolvedores, as máquinas se comunicaram entre si, passando a usar uma linguagem única, criada por elas. In: VAIANO, Bruno. Robôs do Face criam língua própria - mas calma, não é a revolução das máquinas. **Superinteressante**, São Paulo, 1 ago. 2017. Disponível em: https://super.abril.com.br/tecnologia/robos-do-face-criam-lingua-propria-mas-calma-nao-e-a-revolucao-das-maquinas/. Acesso em: 26 jun. 2023.

[37] RIBEIRO, João Luiz Vieira. **Personalização da inteligência artificial**: novo paradigma jurídico. 2020. 300 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito - Centro Universitário de Brasília - UniCEUB, Brasília, 2020.

[38] UNIÃO EUROPEIA, Parlamento Europeu. **Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (2020/2014(INL)).** Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.html. Acesso em: 14 abr.2023.

específico na Resolução, em que especificamente dispõe que não é necessário atribuir personalidade jurídica aos sistemas de IA, *verbis*:

> Responsabilidade e inteligência artificial 7. Observa que todas as atividades, dispositivos ou processos físicos ou virtuais operados por sistemas de IA podem, do ponto de vista técnico, ser a causa direta ou indireta de danos ou prejuízos, contudo são quase sempre o resultado de alguém que construiu, utilizou ou interferiu com esses sistemas; observa, a esse respeito, **que NÃO é necessário conferir personalidade jurídica aos sistemas de IA**; defende que a opacidade, a conectividade e a autonomia dos sistemas de IA podem, na prática, tornar muito difícil, ou mesmo impossível, identificar se determinadas ações danosas dos sistemas de IA tiveram origem numa intervenção humana específica ou em decisões de conceção; recorda que, de acordo com conceitos de responsabilidade amplamente aceites, se pode contornar esse obstáculo atribuindo a responsabilidade às diferentes pessoas da cadeia de valor que criam, fazem a manutenção ou controlam os riscos associados ao sistema de IA.

A solução pela atribuição da personalidade não afasta a necessidade de alcançar o responsável (concreto e apto) para reparar o prejuízo causado ou de encontrar mecanismos subsidiadores dos fundos de indenização, por exemplo.

A questão é que a responsabilidade necessita de patrimônio e, a simples atribuição de personalidade jurídica não outorga patrimônio. Assim, se mostra desnecessário conceder personalidade jurídica aos robôs.

Na segunda parte do trabalho, será abordada a responsabilidade civil por inteligência artificial, no âmbito da União Europeia e, após, a análise do Projeto de Lei acerca do tema, no Brasil. Por fim, será analisado se os dispositivos já existentes na legislação brasileira são suficientes para abarcar os casos de responsabilidade civil relacionados aos sistemas de IA ou se, de fato, haveria necessidade uma legislação específica acerca da temática.

1 Responsabilidade Civil na União Europeia

A proposta da União Europeia acerca da inteligência artificial se baseia em uma regulação escalonada. Uma das premissas da abordagem regulatória é a hierarquização dos riscos (*risk-based regulatory approach*), ou seja, as restrições e exigências aumentam conforme maiores sejam os riscos que os sistemas de IA possam oferecer a direitos e garantias fundamentais dos indivíduos.

Há casos em que há proibição de utilização da IA quando utilizadas para "distorcer o comportamento humano, os quais são passíveis de provocar danos físicos ou psicológicos". Isso porque esses sistemas utilizam "componentes subliminares que não são detetáveis pelos seres humanos ou exploram vulnerabilidades de crianças e adultos associadas à sua idade e às suas incapacidades físicas ou mentais".[39]

O parlamento Europeu entende que a "cobertura da responsabilidade" é um fator relevante para o sucessos das novas tecnologias, bem como os produtos e serviços atrelados. Isso porque estabelece salvaguardas sólidas para os usuários de tais tecnologias. Desse modo, propõe que todos os operados de sistemas IA de alto risco devem ser titulares de seguro que deve abranger os valores indenizatórios.

O Parlamento propõe que deve se atentar que os prêmios de seguro não podem ser proibitivamente elevados para que não seja um obstáculo à inovação. Desse modo, defende que a Comissão da proposta legislativa deve trabalhar de forma conjunta com o setor de seguros, a fim de criar políticas de seguros que tenham ao mesmo tempo preços acessíveis e cobertura adequada[40].

---

[39] UNIÃO EUROPEIA, PARLAMENTO EUROPEU. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2022, Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 09 abr.2023, p. 23.

[40] UNIÃO EUROPEIA, PARLAMENTO EUROPEU. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2022, Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 09 abr.2023, p. 23.

2 Responsabilidade Civil de IA no Brasil

No Brasil havia três projetos de lei sobre inteligência artificial (Projetos de Lei nºs 5.051[41], de 2019, 21[42], de 2020, e 872[43], de 2021), os quais, após amplo debate no Senado Federal[44], foram substituídos pelo no Congresso Nacional, pelo Projeto de Lei n. 2338, de 2023 [45].

No art. 27 da proposta legislativa (n. 2338, de 2023), estabelece expressamente que o "fornecedor ou operador de sistema de inteligência artificial que cause dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema".

Nos casos em que se tratar de sistema de IA de alto risco ou excessivo, "o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano". Na hipótese de não se tratar de sistema de inteligência artificial de alto risco, "a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima".

As hipóteses de exclusão de responsabilidade ocorrerão nos casos de: a) comprovarem que "não colocaram em circulação, empregaram ou tiraram proveito

---

[41] BRASIL. **Projeto de Lei n.5051/2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Disponível em:https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Acesso em: 05 abr.2023.

[42] Cumpre salientar, que na primeira versão desses Projeto de Lei, era pela responsabilidade subjetiva. Uma das críticas era de como seria examinada a culpa, para fins de responsabilização, se a transparência é limitada pelo segredo industrial e comercial, por exemplo. BRASIL. **Projeto de Lei n. 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 05 abr. 2023.

[43] BRASIL. **Projeto de Lei n. 872/2021**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 05 mar.2023.

[44] BRASIL, SENADO FEDERAL. **RELATÓRIO FINAL Comissão de Juristas instituída pelo Ato do Presidente do Senado nº 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil**. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relato%CC%81rio%20final%20CJSUBIA.pdf. Acesso em: 02 abril 2023, p. 80.

[45] BRASIL. **Projeto de Lei nº 2338, de 2023**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1683629462652&disposition=inline&_gl=1*cmo644*_ga*MTQ3NTM0NjAzNS4xNjQ1NTc1MDc1*_ga_CW3ZH25XMK*MTY4MzY3MjcyMS4zLjAuMTY4MzY3MjcyMy4wLjAuMA. Acesso em: 09 abril 2023.

dos sistemas de inteligência artificial"; b) "comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiros, assim como de caso fortuito externo".[46]

Assim, em relação à responsabilidade civil, a opção da proposta legislativa é no sentido de abranger o fornecedor e o operador de sistema de IA evidenciando que sempre que algum desses agentes causar dano patrimonial, moral, individual ou coletivo, será obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema.

Nesse aspecto, adotou-se a gradação de riscos, pois quando se tratar de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida da participação de cada um no dano. E quando se tratar de IA que não seja de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

De salientar que aquelas hipóteses de responsabilização civil oriundas de danos causados no âmbito das relações de consumo, permanecem sujeitas às regras previstas na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), conforme preceitua o art. 29 da referida norma.

3 (Des) Necessidade de regulamentação específica acerca da responsabilidade civil de IA no direito brasileiro?

No "Livro Branco sobre a Inteligência Artificial"[47], de autoria da Comissão Europeia refere que, não obstante a IA traga muitas vantagens é inegável a possibilidade de danos causados, os quais podem ser materiais, quando se referem à saúde, perda de vida e danos à propriedade, por exemplo; e, ainda, imateriais, quando dizem respeito à privacidade e questões discriminatórias.

---

[46] Hipóteses expressamente previstas no art. 28. BRASIL. **Projeto de Lei nº 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial.** Brasília: Senado Federal, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1683629462652&disposition=inline&_gl=1*cmo644*_ga*MTQ3NTM0NjAzNS4xNjQ1NTc1MDc1*_ga_CW3ZH25XMK*MTY4MzY3MjcyMS4zLjAuMTY4MzY3MjcyMy4wLjAuMA. Acesso em: 09 abril 2023.

[47] Comissão Europeia, Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança [COM(2020) Disponível em: https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pt.pdf. Acesso em: 16 abr.2023.

Nesse aspecto, a relevância do estudo do tema, a fim de verificar quem serão os responsáveis acerca de eventual dano, bem como se os mecanismos existentes na legislação brasileira são suficientes ou se, de fato, seria necessária uma abordagem específica.

A questão da regulação específica acerca da responsabilidade civil por sistemas de IA foi amplamente debatida no substitutivo do Senado. Anderson Schreiber (UERJ), entende que o projeto não deveria abordar a questão da responsabilidade, pois teria que especificar várias hipóteses. Caitlin Mulholland (PUC/RJ) e Nelson Rosenvald, entendem pela necessidade de um seguro obrigatório para IA de alto risco. Por sua vez, Fernando Filgueiras (UFG- GOIÁS), entende a necessidade de regular modelos de negócio, ao argumento de que regular IA na saúde é diferente de regular no CADE.[48]

Os renomados doutrinadores Eugênio Facchini Neto e Fábio S. de Andrade entendem pela desnecessidade de regulação específica, porquanto os mecanismos existentes no sistema já são suficientes para abarcar as hipóteses de responsabilidade civil.[49]

O Código Civil Brasileiro possui cláusulas gerais de responsabilidade. Nesse aspecto, abordaremos, inicialmente, as hipóteses em que o próprio Código Civil já poderia resolver essas questões:

A possibilidade de atribuir a responsabilidade objetiva pela atividade de risco de sistemas de IA encontra respaldo no art. 927 do Código Civil, que expressamente dispõe: "aquele que, por ato ilícito (art. 186 e 187), causar dano a outrem, fica obrigado a repará-lo". Haverá obrigação de reparar o dano independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente

[48] Conforme se verifica dos debates ocorridos no âmbito da Comissão de Juristas. BRASIL, SENADO FEDERAL. RELATÓRIO FINAL Comissão de Juristas instituída pelo Ato do Presidente do Senado nº 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil. Disponível em: https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relato%CC%81rio%20final%20CJSUBIA.pdf. Acesso em: 02 abril 2023.

[49] NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71 e ss.

desenvolvida pelo autor do dano implicar, por sua natureza, risco para outrem.[50] O *Codice Civile* italiano estabelece autêntica cláusula geral de responsabilidade para as atividades de risco, em seu art. 2050[51], ao dispor:

> Art. 2050. **Responsabilità per ç'esercizio di attivitá pericolose.** Chiunque cagiona danno ad Altri nello svolgimento di uma attivitá pericolosa, per su natura o per la natura dei mezzi adoperati, é tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.

Alguns doutrinadores denominam a responsabilidade objetiva baseada na teoria do risco, como é chamada nos Estados Unidos de "deep pocket" (bolso profundo). Isso porquanto pessoas que, de alguma forma, estão envolvidas em atividades perigosas e, que ao mesmo tempo produzem algum tipo de proveito, devem compensar o dano causado, sendo atribuída a obrigação de indenizar aquele que "tem maior capacidade financeira de garantir e gerir os riscos e perigos da atividade, adotando seguro contra danos".[52]

Desse modo, há o entendimento de que, em não sendo atribuída a personalidade à IA, ela é um produto e, portanto, se enquadra na responsabilidade pelo fato das coisas, porquanto "o anonimato do autor da lesão e a extensão da responsabilidade a terceiros é a evidência da adequação da responsabilidade objetiva a esse contexto de novas tecnologias".[53]

Nesse ponto, o reconhecimento de atividade de risco a partir do emprego generalizado sistemas de IA "parece ser a solução mais adequada, em linha de

---

[50]TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência Artificial e elementos da responsabilidade Civil. Inteligência Artificial e Direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais, 2019, p. 239-348, p. 317.

[51] Tradução Livre. "Art. 2050. (Responsabilidade pelo exercício de atividade perigosas). Quem causar dano a outras pessoas ao desempenhar uma atividade perigosa, por sua natureza ou pela natureza dos meios utilizados, é responsável pelo ressarcimento, se não provar ter tomado todas as medidas adequadas para evitar o dano." **IN: ITÁLIA. Códice Civile 2023.** Testo del Regio Decreto 16 marzo 1942, n. 262 aggiornato con le modifiche apportate, da ultimo, dalla Legge n. 41/2023. Disponível em:https://www.altalex.com/documents/news/2014/02/19/dei-fatti-illeciti. Acesso em: 1º julho 2023.

[52]MULHOLLAND, Caitlin. Responsabilidade Civil e processos decisórios autônomos em sistemas de inteligência artificial (IA): autonomia, imputabilidade e responsabilidade. Inteligência Artificial e Direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais, 2019, p. 325-348, p. 341.

[53]ANTUNES, Henrique Sousa. Inteligência artificial e responsabilidade civil: enquadramento. **Revista de Direito da Responsabilidade, ano**, v. 1, p. 139-154, 2019.

princípio, para o equacionamento da questão atinente à individualização do critério de imputação do regime de responsabilidade". Todavia, não se pode invocar de maneira indiscriminada e irrefletida da "noção de atividade de risco".[54]

O artigo 936 do Código Civil, que dispõe acerca da responsabilidade civil por fato de animais, preconiza que "o dono, ou detentor, do animal ressarcirá o dano por este causado, se não provar culpa da vítima ou força maior"[55]. Nesse aspecto, os doutrinadores Gustavo Tepedino e Rodrigo da Silva Guia[56] entendem que como a IA não é sujeito, mas "coisa", poderia usar esse dispositivo de forma analógica, para fins legais. Isso porque entendem que tanto os animais, como sistemas autônomos de IA, possuem similar ordem de inteligência a imprevisibilidade.

A responsabilidade por ato de outrem, disposta no art. 932 do Código Civil[57], também chamada de responsabilidade vicária ou *vicarious liability*, também poderia ser aplicada aos sistemas de IA, isso porque o que torna alguém responsável "pelo ato de outrem não seria o fato de ter cometido algum ato ilícito, mas sim sua relação com o autor direto do dano, que poderia ser seu filho, pupilo, curatelado, empregado ou preposto"[58]. Nesse aspecto, o mesmo poderia ser aplicado com o proprietário de

---

[54] TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência Artificial e elementos da responsabilidade civil. **Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais**, 2019, p.293- 348, p. 318.

[55] BRASIL. **Lei n. 10.406/2022**. Lei n.10406, de 10 de Janeiro de 2022. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 abr.2023.

[56] TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência Artificial e elementos da responsabilidade civil. **Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais**, 2019, p.293- 348, p. 315. No mesmo sentido: NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71 e ss.

[57] Art. 932. São também responsáveis pela reparação civil: I - os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia; II - o tutor e o curador, pelos pupilos e curatelados, que se acharem nas mesmas condições; III - o empregador ou comitente, por seus empregados, serviçais e prepostos, no exercício do trabalho que lhes competir, ou em razão dele; IV - os donos de hotéis, hospedarias, casas ou estabelecimentos onde se albergue por dinheiro, mesmo para fins de educação, pelos seus hóspedes, moradores e educandos; V - os que gratuitamente houverem participado nos produtos do crime, até a concorrente quantia. Art. 933. As pessoas indicadas nos incisos I a V do artigo antecedente, ainda que não haja culpa de sua parte, responderão pelos atos praticados pelos terceiros ali referidos. In: BRASIL. **Lei n. 10.406/2022**. Lei n.10406, de 10 de Janeiro de 2022. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 abr.2023.

[58] NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71 e seguintes, p.93.

um artefato dotado de IA, em que o proprietário ou usuário responderiam pela sua ligação com a coisa.

Nesse aspecto, o próprio art. 931 do Código Civil assinala que, ressalvados os casos previstos em lei, "os empresários individuais respondem independentemente de culpa pelos danos causados pelos produtos postos em circulação."[59]

Em casos excepcionais, posição que é minoritária, seria possível atribuir a responsabilidade subjetiva, conforme exemplo trazido pelo jurista Eugenio Facchini Neto, no caso de falha humana, em razão da não atualização do software, conforme determinado pelo fabricante.[60]

No âmbito do Código de Defesa do Consumidor, importante assinalar a responsabilidade pelo fato do produto, prevista no art. 12 do referido diploma legal[61]. Nesse artigo, há uma solidariedade entre os integrantes da cadeia produtiva, porquanto o fabricante, produtor, construtor, importador, em que, independentemente da existência de culpa, todos respondem por danos causados aos consumidores.

Desse modo, os fabricantes de "robôs inteligentes, ou quaisquer outros artefatos dotados de inteligência artificial, são objetivamente responsáveis por quaisquer danos que seus produtos possam causar."[62]

---

[59] BRASIL. **Lei n. 10.406/2022**. Lei n.10406, de 10 de Janeiro de 2022. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 abr.2023.

[60] Conforme exemplo trazido pelo Professor Facchini, o qual restou ser, ainda assim, uma posição minoritária. FACCHINI NETO, Eugênio. "**Inteligencia Artificial y responsabilidade civil**" (palestra), Facultad de Traducción e Interpretación de la Universidad de Granada - Espanha, 27 de janeiro, 2023.

[61] Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos. § 1° O produto é defeituoso quando não oferece a segurança que dele legitimamente se espera, levando-se em consideração as circunstâncias relevantes, entre as quais: I - sua apresentação; II - o uso e os riscos que razoavelmente dele se esperam; III - a época em que foi colocado em circulação. § 2º O produto não é considerado defeituoso pelo fato de outro de melhor qualidade ter sido colocado no mercado. § 3° O fabricante, o construtor, o produtor ou importador só não será responsabilizado quando provar: I - que não colocou o produto no mercado; II - que, embora haja colocado o produto no mercado, o defeito inexiste;III - a culpa exclusiva do consumidor ou de terceiro. BRASIL. **Lei n. 8.078/1990.** Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 abr. 2023.

[62] NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71 e seguintes, p. 95.

Isso porque, tanto o artigo 12 do CDC, como o art. 18, que trata da questão de vício de qualidade, abarca tanto serviços quando produtos. Assim, conforme assinalam os juristas Dr. Fábio S. de Andrade e Dr. Eugênio Facchini Neto[63], a "noção do art. 18 é suficiente abrangente tanto como fator de responsabilidade como de imputação para o fabricante, mesmo que não se prertenda utilizar a noção de defeito".

No âmbito do Código de Defesa do Consumidor, o Ministro Paulo Sanseverino quatro pressupostos da responsabilidade, contidos no art. 12 e 14: o defeito do produto, o nexo de imputação, o dano patrimonial ou extrapatrimonial e a relação de causalidade entre defeito e dano.

Por defeito do produto ou serviço, entende que não oferece a segurança que deles se espera, os tornando perigosos e potencializando-os para a causação de danos ao consumidor. No que atine ao nexo de imputação, assinala que é o "vínculo entre o defeito (produto/serviço) e a atividade desenvolvida pelo fornecedor para a atribuição do dever de indenizar". Quanto ao dano patrimonial ou extrapatrimonial refere ser a "ampla gama de prejuízos causados". No que tange à relação de causalidade entre defeito e dano, assinala que é a relação de "causa e efeito que se estabelece entre defeito (produto/serviço) e dano para reconhecer o acidente de consumo e obrigação de indenizar." [64] Todos esses requisitos poderiam ser utilizados para verificar a responsabilidade de sistemas de IA.

No que atine ao seguro obrigatório e fundo de garantia, embora o país ainda seja deficitário, seria também uma das possibilidades[65].

Cumpre assinalar que, no sistema brasileiro, não há grandes dificuldades na questão atinente ao enquadramento da responsabilidade, em razão do guarda-chuva de opções disponíveis, seja pelas disposições do Código de Defesa do Consumidor, seja pelas opções constantes no Código Civil.

---

[63] NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71 e seguintes, p. 95.

[64] SANSEVERINO, Paulo de Tarso Vieira. **Responsabilidade Civil no Código do Consumidor e a defesa do fornecedor.** 3 ed. São Paulo- Saraiva, 2010, p. 119.

[65] FACCHINI NETO, Eugênio. "**Inteligencia Artificial y responsabilidade civil**" (palestra), Facultad de Traducción e Interpretación de la Universidad de Granada - Espanha, 27 de janeiro, 2023.

Desse modo, tendo em vista a gama de instrumentos no direito brasileiro, tem-se que não seria necessário que uma legislação específica sobre IA tratasse acerca da questão da responsabilidade. O sistema do CDC é de solidariedade e, ainda, temos as cláusulas gerais do Código Civil, os quais abarcariam as questões de responsabilização por danos causados por sistemas de IA.

CONCLUSÃO

Problema delicado, que tem gerado discussões à nível mundial, diz respeito a responsabilidade civil da Inteligência Artificial. Os benefícios de utilização de IA são inegáveis, mas é sempre bom lembrar que sua aplicação pode gerar riscos excessivos para usuários e/ou desenvolvedores. Os governos mundiais têm discutido amplamente uma estrutura regulatória para gerenciar e coibir excessos no uso dessas tecnologias.

No Brasil e no âmbito do Parlamento Europeu, as regulações ainda estão pendentes de aprovação. A diferença do direito brasileiro com o europeu é que, no campo da responsabilidade, temos o Código Civil e o Código de Defesa do Consumidor, que tem os dispositivos necessários para analisar e resolver questões atintes à responsabilidade civil, decorrentes/ ocasionadas por sistemas de inteligência artificial.

Isso porque, o direito brasileiro possui, no CDC, um regime especial bem desenvolvido no que tange ao fato do produto e com um sistema amplo de solidariedade, abarcando todos os participantes da relação do consumo. Ademais, o Código Civil possui cláusulas gerais de responsabilidade, com uma disciplina por produtos perigosos, por exemplo. Também, a responsabilidade por fato da coisa poderia ser adotada, com aprofundamento doutrinário e principiológico, dentre outros.

Uma das questões aventadas, seria a possibilidade de fundos de garantia e seguros obrigatórios para garantia do adimplemento indenizatório, algo que teria que ser melhor trabalho, porquanto ainda é deficitário no ordenamento brasileiro.

Nesse panorama, tem-se que os regramentos já disponibilizados no nosso sistema seriam suficientes para abarcar as hipóteses de responsabilidade. Todavia,

o cenário das discussões do Projeto de Lei nº 2338, de 2023, demonstram que a responsabilidade civil estará abarcada na nova legislação sobre IA.

O objetivo deste trabalho foi tecer algumas notas acerca da IA, demonstrar a importância do tema, enumerando algumas das suas aplicações já inseridas no cotidiano. Outrossim, mencionar a questão, já superada, da personalidade jurídica dos robôs. Ademais, traçar um breve panorama acerca da responsabilidade civil, no âmbito da União Europeia e do Brasil, envolvendo a temática de inteligência artificial, bem como demonstrar que o ordenamento jurídico brasileiro possui opções, seja no Código Civil ou no Código de Defesa do Consumidor, para abarcar as questões envolvendo responsabilidade civil e Inteligência Artificial. Por fim, em razão das inúmeras possibilidades de discussões envolvendo a temática, não se pretendeu esgotar o assunto.

A utilização de sistemas de inteligência artificial se mostram de salutar relevância, mas é preciso recordar que "a aventura da tecnologia impõe, com seus riscos extremos, o risco da reflexão extrema".[66]

É necessário que as legislações acerca da temática não obstaculizem o desenvolvimento tecnológico, mas também direitos fundamentais devem ser respeitados. Assim, a ética, transparência, o respeito aos direitos fundamentais e governança são requisitos fundamentais quando se trata de utilização de sistemas de IA. Por fim, em razão da amplitude do tema, apenas foram trazidos alguns pontos para auxiliar nas discussões acerca da responsabilidade civil e inteligência artificial, inerentes ao Direito no contexto contemporâneo.

REFERÊNCIAS

ANTUNES, Henrique Souza. Inteligência artificial e responsabilidade civil: enquadramento. **Revista de Direito da Responsabilidade**, a.1., p. 139-154. 2019.

BADIA, Ana Lúcia Seifriz**. Danos extrapatrimoniais coletivos e indenização punitiva: uma visão brasileira a partir do direito comparado**. Curitiba: Juruá, 2022.

[66] JONAS, Hans. **O princípio responsabilidade**: ensaio de uma ética para a civilização tecnológica. Tradução original alemã de: Marijane Lisboa, Luiz Barros Montez. Rio de Janeiro: Contraponto/Puc-Rio, 2006. p. 22.

BRASIL, Ministério da Ciência, Tecnologia e Inovações. **Estratégia Brasileira de Inteligência Artificial – EBIA.** Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/inteligencia-artificial. Acesso em: 05 abr. 2023.

BRASIL. Palácio do Planalto. **Lei n. 14.510, de 27 de dezembro de 2022**.Altera a Lei nº 8.080, de 19 de setembro de 1990, para autorizar e disciplinar a prática da telessaúde em todo o território nacional, e a Lei n] 13.146, de 06 de julho de 2015; revoga a Lei nº 13.989, de 15 de abril de 2020. Brasília: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14510.htm#:~:text=LEI%20N%C2%BA%2014.510%2C%20DE%2027,15%20de%20abril%20de%202020. Acesso em: 16 mar.2023.

BRASIL. **Projeto de Lei n. 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 05 abr. 2023.

BRASIL. **Projeto de Lei n.5051/2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/138790. Acesso em: 05 abr. 2023.

BRASIL. **Projeto de Lei n. 872/2021**. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/147434. Acesso em: 05 mar.2023.

BRASIL. **Lei n. 10.406/2022**. Lei n.10406, de 10 de Janeiro de 2022. Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 11 abr.2023.

BRASIL. **Lei n. 8.078/1990.** Lei n. 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 11 abr. 2023.

BRASIL, SENADO FEDERAL. RELATÓRIO FINAL **Comissão de Juristas instituída pelo Ato do Presidente do Senado nº 4, de 2022, destinada a subsidiar a elaboração de minuta de substitutivo para instruir a apreciação dos Projetos de Lei nºs 5.051, de 2019, 21, de 2020, e 872, de 2021, que têm como objetivo estabelecer princípios, regras, diretrizes e fundamentos para regular o desenvolvimento e a aplicação da inteligência artificial no Brasil.**
https://www.stj.jus.br/sites/portalp/SiteAssets/documentos/noticias/Relato%CC%81rio%20final%20CJSUBIA.pdf. Acesso em: 02 abril 2023.

BRASIL, Sociedade Brasileira de Mastologia. **Inteligência Artificial prevê câncer de mama cinco anos antes**. Disponível em: https://www.sbmastologia.com.br/inteligencia-artificial-preve-cancer-de-mama-cinco-anos-antes/. Acesso em: 31 mar.2023.

BRASIL, Conselho Nacional de Justiça. **Resolução nº332, de 21 de agosto de 2020**. **Dispõe sobre a ética, transparência e a governança na produção e no uso da Inteligência Artificial no Poder Judiciário e dá outras providências**. Disponível em:https://www.cnj.jus.br/wp-content/uploads/2020/08/Resolu%C3%A7%C3%A3o-332-IA-Programa%C3%A7%C3%A3o_v4-.pdf. Acesso em: 25 mar. 2023.

BRASIL, Conselho Nacional de Justiça, 2022**. Justiça 4.0: Inteligência artificial está presente na maioria dos tribunais brasileiros**. Disponível em: https://www.cnj.jus.br/justica-4-0-inteligencia-artificial-esta-presente-na-maioria-dos-tribunais-brasileiros/. Acesso em: 18 março 2023.

BRASIL, Senado Federal. Projeto de Lei nº 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1683629462652&disposition=inline&_gl=1*cmo644*_ga*MTQ3NTM0NjAzNS4xNjQ1NTc1MDc1*_ga_CW3ZH25XMK*MTY4MzY3MjcyMS4zLjAuMTY4MzY3MjcyMy4wLjAuMA. Acesso em: 09 maio 2023.

BRASIL, Supremo Tribunal Federal. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=505767&ori=1#:~:text=A%20RAFA%202030%20(Redes%20Artificiais,por%20meio%20de%20comparа%C3%A7%C3%A3o%20sem %C3%A2ntica. Acesso em: 19 maio 2023.

BRASIL, Supremo Tribunal Federal. Ministra Rosa Weber lança robô VitórIA para agrupamento e classificação de processos: a nova ferramenta dará mais celeridade ao andamento processual e resultará em mais segurança jurídica. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=507426&ori=1. Acesso em 19 maio 2023.

BRASIL, Sociedade Brasileira de Mastologia. **Inteligência Artificial prevê câncer de mama cinco anos antes**. Disponível em: https://www.sbmastologia.com.br/inteligencia-artificial-preve-cancer-de-mama-cinco-anos-antes/. Acesso em: 31 março 2023.

BARBA, Patrick et al. Remote telesurgery in humans: a systematic review. **Surgical Endoscopy**, v. 36, n. 5, p. 2771-2777, 2022.

BERNASIUK, Helen Lentz Ribeiro**.** A inteligência artificial e a necessidade de observância de princípios fundamentais: Victor no Supremo Tribunal Federal. p. 169-19. In: CALIENDO, Paulo; ALFF, Hannah Pereira (Orgs.). **Temas atuais de processo tributário**. Porto Alegre: Editora Fundação Fênix, 2022. 437 p. Disponível em:

https://www.fundarfenix.com.br/_files/ugd/9b34d5_e856932e6d1a4c4cb8ee2da47a016f06.pdf . Acesso em 27 mar. 2023.

BRIAN, Christian; GRIFFITHS, Tom. **Algoritmos para viver***:* a ciência exata das decisões humanas. São Paulo: Companhia das Letras, 2017, que se estendem sobre o que são algoritmos às p. 13,14 e 16.

BURRELL, Jenna. How the machine 'thinks': Understanding opacity in machine learning algorithms. **Big data & society**, v. 3, n. 1, p. 2053951715622512, 2016.

BRUXELAS, PARLAMENTO EUROPEU. Regime de Responsabilidade Civil aplicável à Inteligência Artificial. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.html#title1. Acesso em: 15 abr. 2023.

CABRINI, Natália. 6 Tendências da Telemedicina no Brasil em 2022. **Medicina S/A**, [*s.l.*], 03 mai. 2022. Disponível em: https://medicinasa.com.br/6-tendencias-telemedicina/. Acesso em: 15 jun. 2023.

CASTELLS, Manuel. A sociedade em rede: do conhecimento à política. *In*: CASTELLS, Manuel; CARDOSO, Gustavo (Org.). **A sociedade em rede**: do conhecimento à acção política. São Paulo: Paz e Terra, 2000. v. 1

CALIENDO, Paulo. "**Inteligencia Artificial, Tributación, Metaverso**" (palestra), Facultad de Traducción e Interpretación de la Universidad de Granada - Espanha, 24 de janeiro, 2023.

CONTISSA, Giuseppe; GALLI, Frederico; GODANO, Francesco; SARTOR, Galileo**. IL REGOLAMENTO EUROPEO SULL'INTELLIGENZA ARTIFICIALE Analisi informatico-giuridica**. Disponível em: http://www.ilex.it/articles/Volume14/Fascicolo2RegulationOfAI/Contissa_et_al_Proposta_regolamento.pdf. Acesso em 29 mar. 2023.

COMISSÃO EUROPEIA. Grupo Europeu de Ética na Ciência e Novas Tecnologias. **Declaração de Inteligência Artificial, Robótica e Sistemas 'Autônomos'**. Bruxelas, 9 de março de 2018. Disponível em: http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf. Acesso em: 8 abr. 2023.

Comissão Europeia, Livro Branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança [COM(2020) Disponível em:https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pt.pdf. Acesso em: 16 abr.2023.

CONSELHO FEDERAL DE MEDICINA. **Resolução nº 2311/2022**. Regulamenta a cirurgia robótica no Brasil. Brasília: CFM, 2022. Disponível em: https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2022/2311. Acesso em: 31 março 2023.

CNN BRASIL, Economia. **Reino Unido quer responsabilizar montador por acidentes de carros autônomos**. Disponível em: https://www.cnnbrasil.com.br/economia/reino-unido-quer-responsabilizar-montadoras-por-acidentes-de-carros-autonomos/amp/. Acesso em: 16 abr.2023.

DE ANDRADE, Fabio Siebeneichler; FACCIO, Lucas Girardello. Notas sobre a responsabilidade civil pela utilização da inteligência artificial. **DOUTRINA NACIONAL**, v. 46, n. 146, p. 153, 2019.

FAGGIANI, Valentina. La lotta contro il crimine attraverso gli algoritmi: contraddizioni e profili di (in) constituzionalitá dell' applicazione dell' IA ala giustizia penale. In: **Respuesta Institucional y normativa al crime organizado. Perfiles estratégicos para uma lucha eficaz**. Ed. Thomson Reuters (Legal) Limited/ Franciso Javier Garrido Carrillo (Dir.) y Valentina Faggiani (coord.), 2022, p. 245- 281, p. 254.

FERRARI, Isabela; BECKER, Daniel; WOLKART, Erik Navarro. **Arbitrium ex machina***:* panorama, riscos e a necessidade de regulação das decisões informadas por algoritmos. **Revista dos Tribunais**. Vol. 995, p. 635 – 655 (Set / 2018).

FREITAS, Juarez. **Direito e inteligência artificial**: em defesa do humano. Belo Horizonte: Fórum, 2020.

FREIRE, Raquel. **Carro autônomo da Uber atropela e mata mulher nos EUA: Empresa suspendeu todos os testes com carros autônomos na América do Norte.**19/03/2018. Disponível em: https://autoesporte.globo.com/videos/noticia/2018/03/carro-autonomo-da-uber-atropela-e-mata-mulher-nos-eua.ghtml. Acesso em: 16 abr. 2023.

FACCHINI NETO, Eugênio. "**Inteligencia Artificial y responsabilidade civil**" (palestra), Facultad de Traducción e Interpretación de la Universidad de Granada - Espanha, 27 de janeiro, 2023.

FERNÁNDEZ HERNÁNDEZ, Carlos. El proyecto de reglamento de IA debería utilizar um concepto más restrictivo de esta tecnologia y limitar la autorregulación del sector. **Diario La Ley**, Nº 54, Sección Ciberderecho, 11 de Octubre de 2021, **Wolters Kluwer**. Disponível em: https://diariolaley.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1jTAAAkMzUzMTE7Wy1KLizPw8WyMDI0NDA0NDtbz8lNQQF2fb0ryU1LTMvNQUkJLMtEqX_OSQyoJU27TEnOJUtdSk_PxsFJPiYSYAAGMR5eZjAAAAWKE Acesso em: 15 abr. 2023.

GIL MEMBRADO, Cristina. Una nueva era: hacia el robot sanitario autónomo y su encaje en el derecho. **Una nueva era: hacia el robot sanitario autónomo y su encaje en el derecho**, p. 357-399, 2022.

GOMES, Rodrigo Dias de Pinho. Carros autônomos e os desafios impostos pelo ordenamento jurídico: uma breve análise sobre a responsabilidade civil envolvendo veículos inteligentes. **FRAZÃO, Ana; MULHOLLAND, Caitlin. Inteligência Artificial e Direito. São Paulo: Thomson Reuters Brasil**, p. 567-585, 2019.

GRECO, Luis. **Poder de julgar sem responsabilidade de julgador: a impossibilidade jurídica do juiz-robô.** São Paulo: Marcial Pons, 2020.

HOFFMANN-RIEM, Wolfgang. **Teoria Geral do Direito Digital – Transformação Digital**: Desafios para o Direito. Rio de Janeiro: GEN-FORENSE, 2020.

HARTMANN PEIXOTO, Fabiano. Direito e Inteligência Artificial. **Coleção Inteligência Artificial e Jurisdição**. Volume 2. DR.IA. Brasília, 2020. https://orcid.org/0000-0002-6502-9897. ISBN nº 978-65-00-08585-3. Disponível em: www.dria.unb.br. Acesso em: 15 abr. 2023.

ITÁLIA. **Códice Civile 2023.** Testo del Regio Decreto 16 marzo 1942, n. 262 aggiornato con le modifiche apportate, da ultimo, dalla Legge n. 41/2023. Disponível em:https://www.altalex.com/documents/news/2014/02/19/dei-fatti-illeciti. Acesso em: 1º julho 2023.

JONAS, Hans. **O princípio responsabilidade**: ensaio de uma ética para a civilização tecnológica. Tradução original alemã de: Marijane Lisboa, Luiz Barros Montez. Rio de Janeiro: Contraponto/Puc-Rio, 2006.

LAGE, Fernanda de Carvalho. **Manual de inteligência artificial no direito brasileiro**. Salvador: JusPodivm, 2021.

LAGE, Fernanda de Carvalho; PEIXO, Fabiano Hartmann. Inteligência Artificial e Direito: desafios para a regulação do uso da inteligência artificial. IN: PEIXOTO, P. 271.

LOBO, L. C. Inteligência artificial, o Futuro da Medicina e a Educação Médica. **Revista Brasileira De Educação Médica**, [*S.l.*], v. 42, n. 3, p. 3-8, 2018. Disponível em: https://doi.org/10.1590/1981-52712015v42n3RB20180115EDITORIAL1. Acesso em: 15 jan. 2023.

LOBO, L. C. Inteligência Artificial e Medicina. **Revista Brasileira De Educação Médica**, [*S.l.*], v. 41, n. 2, p. 185-193, 2017. Disponível em: https://doi.org/10.1590/1981-52712015v41n2esp. Acesso em: 15 jan. 2023.

MORALES, Hugo M. P. *et al*. COVID-19 in Brazil—Preliminary Analysis of Response Supported by Artificial Intelligence in Municipalities. **Front. Digit**. **Health**, [*s.l.*], v. 3, n. 648585, p. 1-6, jun. 2021. doi: 10.3389/fdgth.2021.648585.

MONTERASTELLI, Alessandra. Enfermeiros robôs, inteligência artificial e os interesses da maioria. Entrevista concedida a Cátia Rizzatti. **Instituto Humanitas Unisinos**, 21 jan. 2022. Disponível em: https://www.ihu.unisinos.br/626135-enfermeiros-robos-inteligencia-artificial-e-os-interesses-da-maioria-entrevista-especial-com-alessandra-monterastelli. Acesso em: 04 maio 2023.

MULHOLLAND, Caitlin. Responsabilidade civil e processos decisórios autônomos em sistemas de Inteligência Artificial (IA): autonomia, imputabilidade e responsabilidade. **Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais**, 2019, p. 325-348.

NETO, Eugênio Facchini; DE ANDRADE, Fábio Siebeneichler. REFLECTIONS ON THE CIVIL LIABILITY MODEL FOR ARTIFICIAL INTELLIGENCE: PERSPECTIVES FOR BRAZILIAN PRIVATE LAW. **Editora Fundação Fênix**, p. 71.

NETO, ELIAS JACOB DE MENEZES. **Análise Preditiva de decisões judiciais com processamento de linguagem natural e aprendizado profundo**. Minicurso no PPGD-Puc Minas. Transmissão via zoom e pelo canal do youtube Dierle Nunes, 28 de setembro de 2022.Disponível: https://www.youtube.com/watch?v=wRcndqZdkbE. Acesso em 19 mar. 2023.

MELO, Ana Karolina Acris et al. **Regulação da Inteligência Artificial: benchmarking de países selecionados. 2022**. Disponível: https://repositorio.enap.gov.br/bitstream/1/7419/1/2022.12.08%20-%20Regula%C3%A7%C3%A3o%20da%20Intelig%C3%AAncia%20Artificial.pdf. Acesso em: 10 abr.2023.

MOHAN, Anmol et al. Telesurgery and robotics: an improved and efficient era. **Cureus**, v. 13, n. 3, 2021.

OECD. **AI Principles overview**. Disponível em: https://oecd.ai/en/ai-principles . Acesso em: 5 abr. 2023.

PORTUGAL, CARTA PORTUGUESA DE DIREITOS HUMANOS NA ERA DIGITAL**. Carta Portuguesa de Direitos Humanos na Era Digital**. Disponível em: https://www.parlamento.pt/Legislacao/Paginas/Educacao_Carta-Portuguesa-de-Direitos-Humanos-na-Era-Digital.aspx. Acesso em 28 mar. 2023.

PUCRS, Inteligência Artificial na Medicina. Inteligência artificial na Medicina: conheça alguns usos da tecnologia "**Hospital São Lucas da Pucrs é o pioneiro nos estudos em Radiologia e Inteligência Artificial"**. Disponível em: https://www.pucrs.br/blog/inteligencia-artificial-na-medicina/. Acesso em 10 abr. 2023.

PARALAMENTO EUROPEU. UNIÃO EUROPEIA. **Resolução do Parlamento Europeu de 16 de fevereiro de 2017**, com recomendações à Comissão de Direito Civil sobre Robótica. Disponível em: https://solene-gerardin.com/16-february-2017-european-parliament-resolution-with-recommendations-to-the-commission-on-civil-law-rules-on-robotics/. Acesso em: 26 março 2023.

PAULO, Guilherme. **Sophia é a primeira robô da história a ter cidadania oficial em um país. 26/10/2017. Disponível em:** https://www.tecmundo.com.br/produto/123533-sophia-primeira-robo-historia-ter-cidadania-oficial-pais.htm. Acesso em: 1º julho 2023.

RIBEIRO, João Luiz Vieira. **Personalização da inteligência artificial**: novo paradigma jurídico. 2020. 300 f. Tese (Doutorado em Direito) – Programa de Pós-Graduação em Direito - Centro Universitário de Brasília - UniCEUB, Brasília, 2020.

RUARO, Regina Linden; REIS, Ludmila Camilo Catão Guimarães. Los retos del desarrollo ético de la Inteligencia Artificial. **Veritas**, v. 65, n. 3, set.-dez. 2020, p. 1-14, p. 05. http://dx.doi.org/10.15448/1984-6746.2020.3.38564. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=8086046. Acesso em: 09 maio 2023.

ROSA, Giovanni Santa. ChatGPT lança API para empresas que querem colocar IA em seus apps. **Tecnoblog**, [*S.l.*], 01 de março de 2023. Disponível em: https://tecnoblog.net/noticias/2023/03/01/chatgpt-lanca-api-para-empresas-que-querem-colocar-ia-em-seus-apps/. Acesso em: 02 mar. 2023.

SANSEVERINO, Paulo de Tarso Vieira. **Responsabilidade Civil no Código do Consumidor e a defesa do fornecedor.** 3 ed. São Paulo- Saraiva, 2010.
SARLET, Ingo Wolfgang. **A eficácia dos Direitos Fundamentais**. 12. ed. Porto Alegre: Livraria do Advogado, 2015.

SILVA, Nilton Correia da. Notas iniciais sobre a evolução dos algoritmos do VICTOR: o primeiro projeto de inteligência artificial em supremas cortes do mundo. In: FERNANDES, Ricardo Vieira de Carvalho; CARVALHO, Angelo Gamba Prata de (Coord.). **Tecnologia jurídica & direito digital: II Congresso Internacional de Direito, Governo e Tecnologia – 2018.** Belo Horizonte: Fórum, 2018. p. 89-94.

SILVA, José Afonso da Silva. **Curso de Direito Constitucional Positivo**. 36. ed. rev. e atual. São Paulo: Malheiros, 2013.

SOLUM, Lawrence B. Legal Personhood for Artificial Intelligences. North Carolina Law Review, vol. 70,1192, p. 1321ss.

TEIXEIRA, João de Fernandes. **O que é inteligência artificial** (recurso eletrônico). Porto Alegre, RS: Editora Fi, 2017.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. Inteligência Artificial e elementos da responsabilidade civil. **Inteligência artificial e direito: ética, regulação e responsabilidade. Editora Revista dos Tribunais**, 2019, p.293- 348.

TURING, Alan. **Discussion on the mind and the computing machine**. 27.out.1949. Disponível em: http://www.turing.org.uk/sources/wmays1.html. Acesso em: 10 abr.2023.

USP, Faculdade de Medicina. **Simpósio Chat GPT na saúde: Impactos no ensino médico, nas pesquisas e nos cuidados com paciente**. Disponível em: https://www.youtube.com/watch?v=6dUBoq4vacM. Acesso em:03 abril 2023.

UNIÃO EUROPEIA, PARLAMENTO EUROPEU. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS. 2022, Bruxelas. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206. Acesso em: 09 abr.2023.

UNIÃO EUROPEIA, Parlamento Europeu. **Resolução do Parlamento Europeu de 16 de fevereiro de 2017**, com recomendações à Comissão de Direito Civil sobre Robótica. Disponível em: https://solene-gerardin.com/16-february-2017-european-parliament-resolution-with-recommendations-to-the-commission-on-civil-law-rules-on-robotics/. Acesso em: 10 abr. 2023.

UNIÃO EUROPEIA, Parlamento Europeu. **Resolução do Parlamento Europeu, de 20 de outubro de 2020, que contém recomendações à Comissão sobre o regime de responsabilidade civil aplicável à inteligência artificial (2020/2014(INL)).** Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2020-0276_PT.html. Acesso em: 14 abr.2023.

UNIÃO EUROPEIA. **A proteção de dados na União Europeia**. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt. Acesso em: 11 de jul. 2021.

UNIÃO EUROPEIA, GDPR. **General Data Protection Regulation**, Disponível em: https://gdpr-info.eu/. Acesso em: 15 abr. 2023.

VENTURA, Duda. **China lança primeira âncora virtual de telejornal, criada por Inteligência Artificial**. Disponível em:https://istoe.com.br/o-avatar-da-noticia/. Acesso em:15 abr. 2023.

WOLKART, Erick Navarro. **Análise econômica e comportamental do processo civil: como promover a cooperação para enfrentar a tragédia da Justiça no processo civil brasileiro**. 2018. 815 f. Tese (Doutorado) – Programa de Pós-graduação em Direito, Universidade do Estado do Rio de Janeiro – UERJ, Rio de Janeiro, 2018. p. 664. Disponível em: https://www.bdtd.uerj.br:8443/handle/1/17363. Acesso em: 07 fev. 2023.

SEGALLA, Amauri. **Fora da curva: os problemas que atrasam a arrancada de veículos autônomos: aumento do número de acidentes, falhas grosseiras de navegação e corte de investimento pela indústria estão entre os entraves**.10/12/2022. Disponível em: https://veja.abril.com.br/tecnologia/fora-da-curva-os-problemas-que-atrasam-a-arrancada-de-veiculos-autonomos/. Acesso em: 15 abr.2023.

MULLINS, Kate. **Na Suíça, Projeto Blue Brain constrói neurônios 3D e regiões cerebrais inteiras apenas com algoritmos matemáticos**. 11/04/2022. Disponível em: https://www.t4h.com.br/noticias/na-suica-projeto-blue-brain-constroi-neuronios-3d-e-regioes-cerebrais-inteiras-apenas-com-algoritmos-matematicos/. Acesso em: 03 abr. 2023.

MIT Technology Review. **A União Europeia quer regulamentar suas ferramentas de Inteligência Artificia**l. Disponível em:https://mittechreview.com.br/a-uniao-europeia-quer-regulamentar-suas-ferramentas-de-inteligencia-artificial-favoritas/. Acesso em: 16 abr. 2023.

NEWELL, Allen. **Unified theories of cognition**. Cambridge: Harvard University Press,1990.

5. COLETA DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO: OS DESAFIOS DA DICOTOMIA NECESSIDADE X EXCESSO

COLLECTION OF PERSONAL DATA IN EMPLOYMENT RELATIONSHIPS: THE CHALLENGES OF THE NECESSITY VS. EXCESS DICHOTOMY

 https://doi.org/10.36592/9786554600712-05

Regina Linden Ruaro[1]

Jacqueline Varella[2]

RESUMO

O objetivo geral do presente artigo consiste em analisar a complexa interseção entre a proteção de dados pessoais e as relações de trabalho no contexto contemporâneo. Destaca-se a crescente digitalização e interconexão das informações, inclusive entre os órgãos públicos coletores, o que levanta questões problemáticas e cruciais sobre privacidade e segurança das informações dos funcionários. A abordagem é pautada no detalhamento prático das hipóteses, bases legais e princípios que devem nortear a coleta de dados na seara do direito do trabalho, explorando-se os desafios decorrentes da necessidade de equilibrar a obtenção de informações para fins legítimos com a garantia dos direitos individuais dos trabalhadores. Além disso, a pesquisa examina e debate o fato de que a Lei Geral de Proteção de Dados (LGPD) no Brasil é, sem sombra de dúvida, o balizador concreto a ser aplicado para mitigar riscos e estabelecer diretrizes claras para a gestão de dados pessoais nas relações de trabalho, em que pese a existência de lacuna na legislação sobre o tema específico do labor. O estudo também aborda as fases contratuais da coleta de dados, passando pelo alerta acerca da observância da prescrição trabalhista quando

---

[1] Professora Titular da Escola de Direito da Pontifícia Universidade Católica do Rio Grande do Sul. Procuradora Federal/AGU aposentada. Doutora em Direito pela Universidad Complutense de Madrid (1993) com título revalidado pela UFRGS e Pós-Doutora pela Universidad San Pablo - CEU de Madri (2006/2008), Estágio Pós-doutoral na Universidade San Pablo - Ceu de Madri (2016) Compõe o Grupo Internacional de Pesquisa "Protección de Datos, Seguridad e Innovación: retos en un mundo global tras el Reglamento Europeu de Protección de datos". Coordenadora no Brasil pela PUCRS/PPGD/PUCRS no Projeto "Identidad Digital, Derechos Fundamentales y Neuroderechos" - Espanha, Projeto PID2020-120373RB-I00, del Programa Estatal de Investigación, Desarrollo e Innovación Orientada a los Retos de la Sociedad, del Ministerio de Ciencia e innovación. Pesqwuisadora parte de la Red Internacional de Investigadores de la la South EU Google Data Governance Chair de la Universidad CEU- San Pablo. Advogada e Consultora Jurídica nas áreas do Direito Administrativo, Direito Digital e da Proteção de Dados Pessoais. Sócia Fundadora do Regina Ruaro Advogados Associados. Dados.

[2] Mestranda em Direito na PUC/RS. Advogada e consultora Trabalhista, *co-funder* do Escritório RRV Advogados Associados. Foi Diretora da SATERGS (Associação dos Advogados Trabalhistas de Empresas no Rio Grande do Sul) gestão 2018/2020. Conselheira em Empresas Privadas. Integrante do Grupo de Pesquisa GTRATEC (Novas Tecnologias, Processo e Relações de Trabalho - PPGD da PUCRS).

do descarte dos dados. Ao concluir, ressalta-se que, diante do volume relevante de dados coletados no ambiente laboral, é de grande importância o desenvolvimento de ferramentas capazes de agregar controle mais específico do tratamento ocorrido nesse campo, como as de *compliance* e governança. A pesquisa, em sua essencialidade bibliográfica, deu-se com o método indutivo, quando da investigação; passando-se ao método analítico por ocasião da escolha das informações e, no momento da confecção deste relatório em forma de artigo científico, utiliza-se novamente o método indutivo.
Palavras-chave: Proteção de dados. Relações de trabalho. LGPD. Hipóteses práticas. Princípios. Bases legais. Prescrição trabalhista. Excesso.

ABSTRACT

The general objective of this article is to analyze the complex intersection between the protection of personal data and employment relationships in the contemporary context. The increasing digitization and interconnection of information, including among public collecting agencies, is highlighted, raising problematic and crucial questions about the privacy and security of employee information. The approach is grounded in the practical detailing of hypotheses, legal bases, and principles that should guide data collection in the realm of employment, exploring the challenges arising from the need to balance the gathering of information for legitimate purposes with the assurance of individual workers' rights. Furthermore, the research examines and discusses the fact that the General Data Protection Law (LGPD) in Brazil is undoubtedly the concrete benchmark to be applied for mitigating risks and establishing clear guidelines for the management of personal data in employment relationships, despite the existence of a gap in legislation regarding the specific subject of labor. The study also addresses the contractual phases of data collection, ranging from raising awareness about compliance with labor prescription during data disposal. In conclusion, given the significant volume of data collected in the workplace, the development of tools capable of providing more specific control over the treatment in this field, such as compliance and governance tools, is of great importance. The research, in its bibliographical essence, followed the inductive method during the investigation; transitioning to the analytical method when selecting information; and, in the creation of this report in the form of a scientific article, employing the inductive method once again.
Keywords: Data protection. Employment relationships. LGPD. Practical hypotheses. Principles. Legal bases. Labor prescription. Excess.

1 INTRODUÇÃO

A economia é hodiernamente dirigida por dados. Eles são cada vez mais processados e valorados como insumos da sociedade contemporânea e equiparados ao petróleo de outros tempos, e *comodities* dos tempos atuais. Por

outro lado, não há como pensar em desenvolvimento de uma economia e da própria sociedade sem pensar em trabalho, produção e, por consequência, nas pessoas envolvidas em tais atividades: trabalhadores, empregadores e representantes das entidades privadas ou de órgãos públicos que, por deveres anexos, têm autorização e direito de acessar os dados gerados pelas relações de trabalho *lato sensu*[3].

O presente estudo propõe-se a discorrer sobre o significativo volume de coleta e tratamento de dados que ocorre mais predominantemente no âmbito das relações de trabalho do que em outras áreas, apresentando em uma divisão temporal do mercado de trabalho no Brasil – antes e depois das conectividades propiciadas pela internet – que sempre houve, na verdade, relevante coleta de dados pessoais dos empregados. Analisaremos, ainda, que apesar da tão aguardada Lei Geral de Proteção de Dados nº 13.709/2018, a mesma é lacunosa especialmente na matéria laboral, exigindo dos atores, na prática das relações de trabalho, que façam as necessárias adequações das previsões legais genéricas, aos casos concretos do labor no dia a dia. Nessa problemática, então, a pesquisa tem o propósito de debater, sem a pretensão de esgotar a matéria, muitas vezes polêmica em sua complexidade: (i) quais são as bases legais que autorizam o tratamento de dados dos empregados, ancorando-se nas mais seguras e específicas, à luz dos princípios que comumente servem de pilares para a coleta em razão do trabalho; (ii) quais são as hipóteses de coleta de dados e seu volume significativo, antes e depois do fenômeno da internet, e todas as fases da relação de emprego em que ocorrem, e suas justificativas, levando ao questionamento sobre a dicotomia entre necessidade e excesso; (iii) quais são os novos conceitos de ambiente de trabalho para fins de coleta de dados dos empregados, sobretudo considerando o mundo digital e cibernético; (iv) a importância do correto descarte das informações colhidas no bojo das relações de trabalhado atentando-se às peculiaridades das prescrições trabalhistas; (v) o perigo da utilização do consentimento como único amparo para coleta de dados nas

[3] "...relação de trabalho é conceito mais amplo do que relação de emprego. Abrange todas as relações jurídicas em que há prestação de trabalho por pessoa natural a outra pessoa, natural ou jurídica, tanto no âmbito do contrato de trabalho (art. 442, da CLT) como, ainda, no de contrato de prestação de serviços (arts. 593 e seguintes do Código Civil), e mesmo no de outros contratos, como os de transporte, mandato, empreitada etc". MALLET, Estevão. **Apontamentos Sobre A Competência Da Justiça Do Trabalho Após E Emenda Constitucional N. 45**. In: Direito, Trabalho e Processo em Transformação. São Paulo, LTR, 2005, p.169-170.

relações que envolvem subordinação e, finalmente, (vi) a definição das funções/papéis do controlador e do operador de dados na LGPD.

Em arremate é levantada a bandeira do *compliance* como alternativa para lidar com os dados pessoais dos titulares de forma precavida e adequada às melhores práticas nas empresas, sem incorrerem em desrespeito aos ditames da legislação.

2 DISTINÇÃO ENTRE RELAÇÃO DE TRABALHO E RELAÇÃO DE EMPREGO PARA DEFINIÇÃO DO VIÉS DO DEBATE

Convém inicialmente diferenciar relação de trabalho e relação de emprego, com o objetivo de identificar qual delas será objeto desta reflexão. Ao longo dos anos, a doutrina tem se dedicado ao debate sobre essa distinção e, quando se consolidava o entendimento de que emprego seria apenas uma das muitas formas de trabalho, a Emenda Constitucional n° 45 de 8 de dezembro de 2004 retomou a cizânia ao trazer o tema da Competência da Justiça do Trabalho. De forma singela, defende-se que a relação de trabalho é o gênero ao qual pertence a espécie, relação de emprego, entre outras. Segundo Carla Teresa Martins Romar [4], esta distinção pode ser bem esclarecida pela seguinte exegese:

> [A] diferença entre relação de emprego e relação de trabalho está no fato de a primeira ser específica e a última ser genérica, ou seja, como relação de trabalho podem ser consideradas todas as relações jurídicas fundadas em uma obrigação de fazer consubstanciada no trabalho humano, enquanto somente existirá relação de emprego quando o trabalho humano se desenvolver de forma não eventual e subordinada, sendo prestado com pessoalidade e mediante remuneração. [5]

---

[4] Doutora e Mestre em Direito do Trabalho pela PUC-SP. Bacharel em Direito pela USP. Perita em relações de trabalho – Organização Internacional do Trabalho (OIT). Professora dos cursos de Graduação, Especialização, Mestrado e Doutorado em Direito do Trabalho da PUC-SP. Vice-Coordenadora do Programa de Pós-Graduação em Direito da PUC-SP. Professora Convidada dos Cursos de Extensão em Direito do Trabalho da Università degli Studi di Roma Tor Vergata. Membro da Associação Iberoamericana de Derecho del Trabajo e de la Seguridad Social. cromar@terra.com.br" (Romar, 30/09/2019).

[5] ROMAR, Carla Teresa Martins. **Direito do Trabalho Esquematizado**. São Paulo, Editora Saraiva, 5.ª ed., 2018.

Este estudo versará sobre a proteção de dados na relação de emprego, *strictu sensu*, com agentes perfeitamente identificados, em especial o trabalhador (empregado) e o empregador, embora a referência à expressão relação de trabalho *lato sensu,* ao longo do texto, não esteja equivocada, se considerada em seu gênero.

Cumpre destacar, no entanto, que as empresas deverão também fazer adequações não somente para aqueles que tem o vínculo empregatício, configurado na disposição do artigo 3º da Consolidação das Leis do Trabalho e que se baseia na subordinação, habitualidade, pessoalidade e mediante remuneração, mas para todos os tipos de relações de trabalho mantidas no estabelecimento – avulso, estagiário, temporário, terceirizado, etc. –, seja realizada de modo físico ou digital. Contudo, o foco do presente estudo será a abordagem das relações entre empregado e empregador.

Para fins específicos de análise da Lei Geral de Proteção de Dados, é relevante, por fim, explicitar que o empregado é o titular dos dados pessoais que serão objeto de tratamento, e o empregador corresponde ao controlador, que é a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais.[6]

3 DIVISÃO TEMPORAL DA COLETA DE DADOS PESSOAIS DOS EMPREGADOS NO BRASIL, ANTES E DEPOIS DO FENÔMENO DA INTERNET

Dentro desta esfera de relações, em todos os marcos históricos do mercado de trabalho no Brasil, há registros de coleta de dados de empregados e, mais do que isso, há tratamento de dados de forma considerável, incluindo dados pessoais sensíveis. Desta forma, identifica-se que tais relações de emprego merecem significativamente mais atenção se comparadas à outras relações, ao abrigo da Lei nº 13.709/2018.

---

[6] ALVES, Amauri César; ESTRELA, Catarina Galvão. Consentimento do trabalhador para o tratamento de seus dados pelo empregador: análise da subordinação jurídica, da higidez da manifestação de vontade e da vulnerabilidade do trabalhador no contexto da LGDP. **Revista Síntese**: Trabalhista e Previdenciária, São Paulo, v. 31, n. 375, p. 25-40, set. 2020.

3.1 ANTES DA INTERNET

Em momentos anteriores à evolução tecnológica hoje vivida, já se coletavam dados dos empregados em um universo individual, junto aos empregadores, e de forma coletiva, pelas mãos do Governo, cuja justificava era a busca de informações para desenvolvimento de políticas econômicas e sociais e para o preenchimento de vagas de emprego, nas seguintes hipóteses:

(i) quando da realização da Carteira de Trabalho e Previdência Social (Decreto 22.035/1932), foi o primeiro registro de regularização de direitos trabalhistas no nosso país, por meio do qual dados de empregados passaram a ser coletados, armazenados e compartilhados com o Governo Federal para fins estatísticos e, mais recentemente, para acesso a alguns dos mais relevantes direitos sociais, como seguro-desemprego, benefícios previdenciários, Fundo de Garantia do Tempo de Serviço (FGTS), Programa de Integração Social (PIS), entre outros;

(ii) quando da inscrição do trabalhador na RAIS (Relação Anual de Informações Sociais) como ato obrigatório das empresas/empregadores (Decreto nº. 76.900/1975), alimentava uma cadeia produtiva contendo uma gama de dados e informações estatísticas dos trabalhadores, para as decisões governamentais e para gerar dados para sistemas como o Cadastro Geral de Empregados e Desempregados (CAGED), seguro-desemprego, abono salarial, Programa de Integração Social (PIS), Programa de Formação do Patrimônio do Servidor Público (PASEP), Fundo de Garantia do Tempo de Serviço (FGTS) e para sistemas do IBGE, INSS, entre outros. O CAGED e a RAIS foram atualmente atingidos por uma Portaria publicada pelo Governo Federal e que foi responsável por substituí-los pelo e-Social.[7]

[7] PORTARIA SEPRT nº 1127 de 14/10/2019. Define as datas e condições em que as obrigações de prestação de informações pelo empregador nos sistemas CAGED e RAIS serão substituídas pelo Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas - eSocial. (Processo nº 19965.103323/2019-01). **LEGISWEB**. 2019. Disponível em: https://www.legisweb.com.br/legislacao/?id=383471. Acesso em: 01 mai. 2023.

3.2 DEPOIS DA INTERNET

No âmbito coletivo e governamental, a coleta de dados em massa se desenvolveu, se ampliou e se capacitou com a aparição de diversos sistemas complexos de captura, que ocorreram quando da criação do e-Social - Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (Decreto nº 8373/2014)[8]. Trata-se de sistema desenvolvido pelo governo brasileiro para unificar a coleta de informações fiscais, trabalhistas e previdenciárias das empresas. Tem como foco visualizar o cumprimento das obrigações legais pelos empregadores, mas trabalhando com dados dos empregados, ou seja, de vínculos empregatícios, das contribuições previdenciárias, da folha de pagamento, das comunicações de acidente de trabalho, aviso prévio, escriturações fiscais, captura de diversas informações (dados pessoais) dos trabalhadores, bem como informações sobre o FGTS, entre outros. Atualmente, sem o tratamento dessas informações, o Governo Federal não teria meios para desenvolver suas políticas sociais, tampouco exercer seu poder regulatório e de controle, estando refém desse sistema para projeções administrativas, financeiras e políticas, sobretudo.

Já na esfera individual, a coleta de dados igualmente se intensificou e se tornou mais complexa, vez que as informações que antes eram obtidas mediante uma singela entrevista prévia à contratação (e no universo restrito da execução do contrato de trabalho) acabaram indo ao mundo.

Atualmente o trabalhador, antes de chegar a ser candidato a uma vaga de trabalho, já é (a) rastreado por algoritmos para formação de perfil profissional, na pré-contratação, e (b) rastreado depois, durante o desenvolvimento da relação pactual de emprego, sobretudo quando usa as suas próprias interfaces (tablets,

---

[8] O projeto eSocial é uma ação conjunta dos seguintes órgãos e entidades do governo federal: Secretaria da Receita Federal do Brasil – RFB, Caixa Econômica Federal, Instituto Nacional do Seguro Social – INSS e Ministério do Trabalho – MTb. A implantação do eSocial viabilizará garantia aos diretos previdenciários e trabalhistas, racionalizará e simplificará o cumprimento de obrigações, eliminará a redundância nas informações prestadas pelas pessoas físicas e jurídicas, e aprimorará a qualidade das informações das relações de trabalho, previdenciárias e tributárias. A legislação prevê ainda tratamento diferenciado às micro e pequenas empresas. (ESOCIAL. O Decreto nº 8373/2014 instituiu o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial). **SPED** (Sistema Público De Escrituração Digital). Disponível em: http://sped.rfb.gov.br/pagina/show/1507#:~:text=O%20Decreto%20n%C2%BA%208373%2F2014,Previdenci%C3%A1rias%20e%20Trabalhistas%20(eSocial). Acesso em 01 mai. 2023).

smarthphones, notebook) dentro do ambiente de trabalho e eventualmente se expõe em redes sociais públicas, como se explicitará adiante.

4 DADOS PESSOAIS E AS BASES LEGAIS PARA TRATAMENTO

Com o intuito de analisar as necessárias adequações que devem ser feitas entre a Lei Geral de Proteção de Dados Pessoais e o tratamento de dados pessoais nas relações empregatícias, é necessário estudar antes as bases legais que os respaldam.

3.3 SUPERANDO O DEBATE SOBRE A APLICAÇÃO DA LGPD ESPECIFICAMENTE NAS RELAÇÕES DE TRABALHO

Em análise apriorística das diretrizes da Lei nº 13.709/2018, logo se verifica que não há registro das palavras “emprego” ou “trabalho” ao longo de seu corpo textual normativo. Entretanto, o art. 3º estabelece que a LGPD é aplicada a qualquer tipo de tratamento, inclusive o realizado por pessoa jurídica de direito privado, inferindo-se, portanto, que não há óbice para que incida o fato, na norma em questão, considerando-se como o fato o manuseio de dados de trabalhadores, enquanto titulares, por empresas empregadoras, na condição de controladoras.

Ademais, havendo sido, no artigo 4º da Lei, expressamente elencadas as hipóteses excludentes de sua aplicação, fica clara que as relações de trabalho não estão ali inseridas, o que vem corroborado pela aplicação do art. 8º da CLT que firma verdadeira cláusula de abertura, autorizando o diálogo entre as fontes trabalhistas e o direito comum, em caráter subsidiário – o que, por óbvio, inclui a Lei Geral de Proteção de Dados Pessoais.

Finalmente, a atual Carta Magna, ao versar sobre regras de competência *ratione materiae* da Justiça do Trabalho, estabelece que é atribuição dessa Especializada julgar temas oriundos da relação de trabalho. Por conseguinte, as controvérsias que envolvam o tratamento de dados pessoais de obreiros (que são os titulares) por seus empregadores (que são os controladores) devem ser atraídas para essa jurisdição laboral, principalmente quando envolvem dados produzidos em

decorrência do trabalho propriamente dito. Conclui-se, portanto, que é plenamente possível, com as devidas adaptações, a aplicação da LGPD às relações de emprego.

3.4 HIPÓTESES DE AUTORIZAÇÃO DE TRATAMENTO DE DADOS PESSOAIS DOS EMPREGADOS E OS PRINCÍPIOS QUE O REGEM

A LGPD autoriza o tratamento de dados pessoais em artigo 7º em 10 (dez) hipóteses, sendo que, normalmente, as bases legais utilizadas nas relações de trabalho são cerca de 03 (três) delas[9], previstas nos incisos II, V e VI do dispositivo citado, a saber: (a) para cumprimento de obrigação legal a que se sujeita o controlador. Exemplo: preenchimento do e-Social; (b) para execução do contrato de trabalho, do qual é parte o empregado, ou procedimentos prévios ao contrato. Exemplo: informações médicas passadas para planos de saúde, assim como, informações religiosas para inclusão em contratos que exigem trabalho aos sábados, o que não é admitido por algumas religiões, e; (c) para o exercício regular de direitos em processos judiciais, administrativos e arbitrais. Exemplo: defesa da empresa em ações trabalhistas ou previdenciárias.

Essas hipóteses permissivas (artigo 6º, incisos I ao III) devem estar inseridas na fatoração trinômica que passamos neste estudo a chamar de FAN (finalidade, adequação e necessidade[10]), e que se alinham ao princípio da minimização dos dados, que obriga o empregador a observar, no tratamento de dados, somente

---

[9] MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **As Bases Legais de Tratamento de Dados no Ambiente de Trabalho**: Análise da Adequação Entre a LGPD e a Lei Trabalhista. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo (SP): Editora Revista dos Tribunais. 2022. Ebook, Disponível em: https://www.jusbrasil.com.br/doutrina/reflexos-da-lgpd-no-direito-e-no-processo-do-trabalho/1590440816. Acesso em: 1 mai. 2023.

[10] Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

aqueles que são estritamente adequados e necessários ao desenvolvimento e à finalidade das atividades do empregado no contexto da relação de emprego.

3.5 QUAIS DADOS PESSOAIS E QUAIS DADOS PESSOAIS SENSÍVEIS SÃO COLHIDOS NA RELAÇÃO DE EMPREGO E QUAIS PODEM SER TRATADOS?

3.5.1 Tipos de dados colhidos nas relações de trabalho na prática e suas fases de coleta/tratamento

Não há como não se preocupar com a quantidade e variedade de informações dos empregados que estão presentes em arquivos de empresas (físicos ou eletrônicos) que, em tese, os empregadores sempre encontram uma justificativa (ou não) para serem colhidos, como as dos exemplos abaixo elencados, sejam dados pessoais e/ou dados pessoais sensíveis, em conjunto:

(i) nome, estado civil, residência, filiação, idade, e-mail, telefone, R.G., CPF e comprovante de escolaridade fazem parte normalmente dos cadastros dos contratos de trabalho, sendo necessárias para a execução do pacto;

(ii) dados de cônjuges ou companheiros e de filhos são coletados entre outras causas legais (a) para fins de identificação de herdeiros junto ao INSS; (b) pagamento de obrigações legais relacionadas aos salário maternidade/paternidade e apuração de cotas para pagamento de salário família; (c) como o pagamento de pensão, inclusão de dependente no plano de saúde, entre outros;

(iii) dados de imagem justificam-se para a confecção de crachá ou monitoramento de segurança do ambiente, podendo ser justificados como necessárias à execução do contrato e proteção à vida;

(iv) dados biométricos justificam-se para ingresso nos locais de trabalho e anotação dos horários de trabalho, em cumprimento às obrigações legais de controle de jornada dos empregados (registros de ponto eletrônico) e execução do contrato;

(v) dados de filiação à sindicato, dados salariais e bancários justificam-se em face dos atuais mecanismos de pagamento dos salários (crédito em contracorrente ou conta-salário), aos procedimentos em relação à folha de pagamento de responsabilidade do empregador (inclusive eventuais descontos à entidade sindical),

hipóteses todas em que poderá haver compartilhamento com terceiros, sejam escritórios de contabilidade, bancos ou Entidades Sindicais, podendo ser justificadas pela necessidade de obrigação legal e tutela da saúde, bem como cumprimento de normas coletivas;

(vi) dados de desempenho profissional justificam-se para políticas salariais, de promoção e merecimento e eventualmente até de desligamento, bem como para cumprir obrigação legal de demonstrar legitimidade das decisões empresariais, estruturas piramidais e afastamento de equiparações salariais na forma da legislação trabalhista;

(vii) dados de saúde justificam-se pela obrigação legal do empregador em colher (a) exames admissionais, periódicos e demissionais, (b) dados de tipo sanguíneo e outros (inerentes a esses exames); (c) motivos das faltas justificadas na forma da lei; (d) doenças e acidentes que podem ter origem na natureza das atividades desempenhadas ou nas eventuais condições inadequadas do meio ambiente laboral; (e) outros dados de saúde são também coletados quando oriundos da entrega de atestados médicos diversos pelos empregados aos empregadores, contendo CID ou não; (f) são também compartilhados com terceiros quando relacionados a planos de saúde, justificando-se o tratamento também, nessa hipótese, na tutela da saúde, cumprimento de lei e execução do contrato;

(viii) dados eleitorais são coletados geralmente para apuração de efeitos nos dias trabalhados (folgas compensatórias pelo trabalho nas eleições, etc) e cumprimento das obrigações legais com as jornadas laborais;

(ix) dados do certificado de alistamento militar ou reservista podem ser coletados apenas para verificação do cumprimento da obrigação legal de alistamento, mas geralmente sem conexão com a finalidade, adequação e necessidade do contrato de trabalho;

(x) dados de opção sexual justificam-se quando há pedido individual ou ordem judicial de troca de nome em documentos oficiais, em função de troca de gênero, em cumprimento às leis e decisões judiciais nessa esfera.

O contrassenso reside no fato de que, diante dessa enorme gama de informações normalmente colhidas pelo empregador/controlador, o texto do artigo

13 da CLT obriga o empregado a exibir apenas e tão somente a sua CTPS e, ao menos em tese, os dados ali presentes para perfectibilização da relação de emprego.

Com efeito, fica evidente, então, que nos departamentos pessoais das empresas há a coleta de inúmeros dados sensíveis de empregados, por vezes se afastando do princípio basilar da minimização dos dados, que inclusive são colhidos em abundância em pelo menos três fases da relação contratual havida entre essas partes, como vemos adiante.

3.5.2 Coleta de dados na fase pré-contratual - recrutamento e seleção

O momento de seleção de candidatos e o processo adequado de recrutamento merece atenção, pois podem ser coletados dados pessoais que extrapolam a fatoração trinômica que nesta pesquisa se denominou de FAN (finalidade, adequação e necessidade), por exemplo:

(i) dados de antecedentes criminais. A exigência de certidão de antecedentes criminais já foi objeto de decisão do Tribunal Superior do Trabalho (TST), em acórdão publicado em 22/09/2017, no julgamento do Recurso Repetitivo (RR) 243000-58.2013.5.13.0023[11], com a fixação da tese jurídica prevalecente em que a exigência de certidões de antecedentes criminais somente se justifica em casos excepcionais: em virtude (a) da existência de lei, (b) da natureza do ofício ou (c) do elevado grau de fidúcia exigido para a função. Há situações que poderiam justificar o pedido, a ser avaliado no caso concreto: empregados domésticos, cuidadores de menores, idosos ou deficientes (em creches, asilos ou intuições afins), motoristas rodoviários de carga, empregados que laboram no setor da agroindústria no manejo de ferramentas de trabalho perfurocortantes, trabalhadores que atuam com substâncias tóxicas, entorpecentes e armas e trabalhadores que atuam com informações sigilosas. Ainda assim, o tema não é uníssimo, haja vista que, na decisão acima, foram vencidos parcialmente os Ministros Augusto César de Carvalho, relator, Aloysio Corrêa da Veiga, Walmir Oliveira da Costa e Cláudio Mascarenhas Brandão. Os operadores de

[11] BRASIL. Tribunal Superior do Trabalho. **RR: 2430005820135130023**. Recurso de revista. Processo representativo da controvérsia do incidente de recursos repetitivos - tema nº 1. Exigência de certidão de antecedentes criminais de candidatos a emprego. Indenização por dano moral. Relator: Márcio Eurico Vitral Amaro, 30 mai. 2016.

telemarketing foram incluídos por decisões reiteradas dos Tribunais Trabalhistas como trabalhadores que lidam com informações sigilosas, na medida em que atuam diariamente com intenso fluxo de dados, sendo, assim, justificável a exigência à luz da jurisprudência da SBDI-1 do C.TST; [12]

(ii) testes psicotécnicos não deveriam ser realizados ou exigidos, exceto quando há exigência legal ou os justifiquem o trinômio FAN (finalidade, adequação e necessidade) ou outros previstos na LGPD, relacionados por exemplo à saúde e à vida de terceiros;

(iii) análises médicas sobre saúde ou gravidez são inadmissíveis de serem captadas, pois podem implicar na negativa de admissão ou, no mínimo, gerar preconceito e estigma, proibidos por lei;

(iv) gravação de entrevistas de seleção, ao menos em princípio, sempre deveria ser expressamente consentidas antes de sua realização;

(v) histórico comercial é proibido exceto no caso de trabalhadores com poderes de cargo de confiança, ou para representar o empregador, como gerentes, gerentes adjuntos, agentes ou advogados, desde que, em todos esses casos, sejam dotados, pelo menos, de poderes de administração. Também é permitido no caso de trabalhadores encarregados da cobrança, administração ou custódia de fundos ou valores mobiliários de qualquer natureza;13

(vi) checagem de antecedentes técnicos e pessoais (*Background Checks e Pre-employment vetting*) são termos que remetem ao processo de verificação dos antecedentes de trabalhadores e/ou candidatos a uma vaga de emprego, que pode ser feito por algoritmos ou por outros empregados ou empresas terceirizadas contratadas para tanto. A finalidade seria averiguar, entre tantas questões, as que seguem: (a) adequação do candidato à cultura da empresa; (b) se seu currículo agrega valor à atividade empresarial desenvolvida; (c) se suas habilidades são compatíveis com as exigências do cargo; (d) se há confirmação do histórico de emprego; (e) se as credenciais técnicas, educacionais e de experiência prática são

---

[12] BRASIL. **E-ED-RR – 182000-05.2013.5.13.0008**. Relatora Ministra: Maria Cristina Irigoyen Peduzzi, Subseção I Especializada em Dissídios Individuais, 24 mai. 2018.

[13] ALCASSA, Flávia. A Lei Geral de Proteção de Dados Pessoais (LGPD) E A Exposição de Dados Sensíveis Nas Relações de Trabalho. **Revista Síntese**: Trabalhista e Previdenciária. Rev. do Trib. Reg. Trab. 10ª Região, Brasília, v. 24, n. 2, p. 145-51, 2020.

autênticas, como diplomas, certificados, reconhecimentos e premiações profissionais; (f) verificação de perfis de mídia social para alinhamentos culturais e profissionais. Nesses casos é fundamental que as políticas de verificação estabeleçam diretrizes e protocolos claros, a fim de que se observem as melhores práticas, inclusive para prova de que a triagem tem um padrão que garanta isonomia e não discriminação14 entre os candidatos. Esse processo de triagem de dados de candidatos poderia estar relacionado com a questão da segurança (*safety)*, conformidade legal (*legal compliance*) e responsabilidade (*liability issues*);

(vii) Busca de Dados de litígios judiciais do candidato – Escavador e outras ferramentas de busca de informações. A consulta pública às ações trabalhistas e criminais só é permitida nos sistemas e portais da Justiça, a partir do número do processo. Isso porque a Resolução 121/2010 do Conselho Nacional de Justiça e a Resolução 139/2014 do Conselho Superior da Justiça Trabalhista impedem o uso de recursos tecnológicos para consulta ampla e irrestrita desses tipos de processos, com base no nome ou em outros dados pessoais das pessoas envolvidas na ação. O objetivo é evitar a formação de "listas sujas" de trabalhadores que processaram empregadores ou qualquer outra forma de discriminação. A tratativa do assunto está sendo realizada no Recurso Extraordinário com Agravo (ARE) 1307386, em que o site Escavador solicita que o STF fixe uma tese jurídica nacional, baseada em decisão proferida pelo Tribunal de Justiça do Rio Grande do Sul (TJ-RS) favorável ao portal.15

Isso ocorreu porque o Tribunal Regional julgou improcedente o pedido de indenização feito por cidadão que teve informações sobre uma reclamação

---

[14] A LGPD, em sintonia com outras legislações, como exemplo com a Lei n. 9.029/1995, prevê que não é possível haver discriminação, inclusive no momento pré-contratual. Então, os recrutadores deverão avaliar a adequação da vaga aos candidatos, de forma objetiva, sem que peçam ou busquem, ainda que informalmente, dados que possam discriminar os pretensos trabalhadores. (JUNIOR, Carlos Augusto Pinto de Vasconcellos; FERREIRA, Victor Silva. Impacto da lei geral de proteção de dados pessoais nas relações de trabalho: a necessidade de implantação do programa de integridade (Compliance). **UERJ Labuta**. 21 de março de 2020. Disponível em: https://uerjlabuta.com/2020/03/21/impacto-da-lei-geral-de-protecao-de-dados-pessoais-nas-relacoes-detrabalho-a-necessidade-de-implantacao-do-programa-de-integridade-Compliance/. Acesso em: 20 de abril.2023).

[15] MECANISMOS de pesquisa que permitem acesso à ações criminais e trabalhistas a partir da consulta de dados pessoais viola LGPD, entenda. **IAPP** (International Association of Privacy Professionals). Disponível em: https://www.lgpdbrasil.com.br/mecanismos-de-pesquisa-que-permitem-acesso-a-acoes-criminais-e-trabalhistas-a-partir-da-consulta-de-dados-pessoais-viola-lgpd-entenda/. Acesso em: 2 mai. 2023.

trabalhista, por ele ajuizada, divulgada pelas páginas de busca do Google e Escavador, a partir da consulta de seus dados pessoais, sob o fundamento de que seria lícita a exposição de processos por sites de conteúdos judiciais que não estejam em segredo de justiça. Aproveitando-se dessa decisão favorável na instância de origem, a parte vencedora (Escavador) recorre ao Supremo para tentar obter uma decisão com efeitos mais amplos, e assim utilizá-la em âmbito nacional.

Embora seja uma realidade que algumas empresas utilizam informações coletadas em banco de dados diversos, para traçar o perfil do candidato e, com base nessas informações, exclusivamente, direcionar suas contratações, o fato é que essa ampla exposição de informações coletadas das mais variadas formas, inclusive pelos sites de buscas, infringe a Lei Geral de Proteção de Dados e pode acarretar, no caso concreto, danos ao seu titular.

3.5.3 Coleta de dados na constância da fase contratual e a nova compreensão do conceito de ambiente de trabalho

Para além da compreensão comum de coleta dos dados citados no item 4.3.1, há uma necessidade atual de que a compreensão do meio ambiente de trabalho seja dinâmica e abranja um conceito espacial, inclusive sob um aspecto artificial (ciberespaço)[16], onde o trabalhador desenvolve as suas atividades com uso de tecnologias, o que tem conferido desafios ao Direito do Trabalho, porque vem alterando, inclusive, a dinâmica da relação empregatícia.

O uso e fornecimento de dispositivos digitais como computadores, notebooks, smartphones, tablets, discos externos portáteis, dentre outros equipamentos, ampliaram o ambiente de trabalho para além dos estabelecimentos físicos das lojas, fábricas e escritórios. Ademais, em algumas situações, passam a vincular o trabalhador 24 (vinte e quatro) horas por dia à atividade profissional,

[16] Sobre o conceito de ciberespaço: "Percebe-se, desse modo, que o ciberespaço é um mundo virtual, capaz de envolver todas as informações existentes no planeta, interagidas pelo usuário. É possível, por meio do ciberespaço, comunicar e trocar informações com um número indeterminado de usuários, de e para qualquer lugar do mundo." (FINCATO, Denise Pires; BITENCOURT, Manoela de. Ciber como Local de Trabalho: o problema (ou a solução?) do teletrabalho transnacional. **Quaestio Iuris**, Rio de Janeiro, v. 08, n. 04, p. 2237-2263, 2015).

independentemente de estar com a família ou amigos em ambiente de lazer, cultura ou de cunho religioso.[17]

Assim, também se ampliou significativamente a possibilidade de monitoramento do empregado por diversas formas, tais como: (a) vídeo-vigilância; (b) geolocalização; (c) monitoramento de contas de e-mail corporativas; e (d) monitoramento de dados dos equipamentos para auxílio na tomada de decisões automatizadas e de cunho comercial, que trazem aos empregadores oportunidades de coleta de dados dos empregados, porém, ao mesmo tempo, oferecem riscos relacionados ao tratamento de dados pessoais daqueles.

Um exemplo disso é a política de *Bring Your Own Device* (BYOD), que significa "traga seu próprio dispositivo" que consiste em uma política adotada pelas empresas para que os empregados utilizem os seus próprios dispositivos (notebooks, tablets e smartphones) para acessar dados e sistemas do empregador para desempenhar suas funções. Neste sentido:

> O fenômeno BYOD surgiu no Brasil em meados de 2011 e é possível afirmar que foi impulsionado por fatores como o surgimento e expansão da computação móvel, a facilidade de aquisição de novas tecnologias e o ingresso da população jovem no mercado de trabalho, já adepta das chamadas novas tecnologias, gerenciando suas vidas a partir de seus dispositivos móveis e aplicativos. Torna-se inevitável reconhecer que esses trabalhadores-consumidores levam para o ambiente profissional seu modo de vida, onde se inserem seus equipamentos pessoais. [18]

As variantes dessa política são as *Bring Your Own Network* (BYON), Traga a sua Própria Rede, e *Bring Your Own Cloud* (BYOC), Traga a sua Própria Nuvem. Isso afeta o relacionamento travado entre empregador e empregado, ditando a necessidade de elaboração de novas cláusulas contratuais que estejam atentas à

---

[17] ARAÚJO JÚNIOR, Francisco Milton. **Parâmetros Para Delimitação Do Meio Ambiente Do Trabalho Na Volatividade Da Sociedade Contemporânea (Ciberespaço)**. *In*: FELICIANO, Guilherme Guimarães. Direito ambiental do trabalho: apontamentos para uma teoria geral. São Paulo: LTr, p. 41-47, 2017, p. 44.

[18] FINCATO, Denise Pires; FRANK, Marina Silveira. Bring Your Own Device (BYOD) e suas Implicações nas Relações de Emprego: reflexões práticas. **Revista Magister de Direito do Trabalho**, São Paulo, v. 15, n. 89, p. 17-35, mar./abr. 2019, p. 19

temática do direito digital e à própria Lei Geral de Proteção de Dados porque “os riscos e as oportunidades deverão fazer parte da estratégia negocial empresarial”[19].

É necessário, assim, na constância do pacto de emprego, o respeito aos direitos fundamentais à privacidade, à intimidade e à proteção de dados, em prejuízo à autodeterminação informativa, devendo prevalecer o valor da necessidade justificadora da coleta de dados, sobre o apetite excessivo, estatístico e explorador da vida do trabalhador.

3.5.4 Término do contrato de trabalho e a necessidade de eliminação dos dados – prazos prescricionais típicos das relações de trabalho

O término do tratamento de dados tem uma importância digna de destaque: é preciso que o empregador saiba até que momento estaria autorizado a continuar o tratamento dos dados pessoais para fazer a sua devida gestão e final eliminação.

Na fase pós-contratual da relação de emprego, na qual finda o vínculo do trabalhador com o empregador, destaca-se que a rescisão pode ocorrer de diversas formas, como despedida por justa causa, dispensa sem justo motivo por iniciativa do empregador e pedido de demissão, o que inclusive afetará a data de efetivo término do contrato. Diante desse panorama, surge o seguinte questionamento: afinal, qual é o tempo permitido para armazenamento de dados pessoais de empregados por parte de seus empregadores, após o término da relação de emprego?

Há diversos dispositivos, inclusive constitucionais, que determinam o armazenamento de dados, como recibos de pagamento de salários, folhas de pagamentos, livros de registro de empregados, exames médicos admissionais, periódicos e demissionais, por 3 (três), 5 (cinco) e até 30 (trinta) anos, como o de FGTS, por exemplo. Paralelamente, os empregadores precisam se atentar ao disposto nos arts. 15 e seguintes da Lei Geral de Proteção de Dados, que prevê as hipóteses para o término do tratamento de dados, situação que ensejará a sua

---

[19] GULARTE, Caroline de Melo Lima. **A Proteção de Dados Pessoais no Uso de Tecnologia na Relação de Emprego**: efeitos do compliance trabalhista digital nas negociações coletivas. Dissertação (Programa de pós-graduação em Direito) – PUCRS, 2020. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/9306. Acesso em: 6 set. 2023, p. 34.

completa eliminação de forma automática, dispensando qualquer solicitação por escrito.

Neste momento de encerramento do pacto de emprego, voltam ao centro do palco os princípios que nesta pesquisa chamamos de FAN (finalidade, adequação, necessidade) e, também, o princípio da transparência, o qual prevê que é obrigação do controlador assegurar a proteção dos dados tratados de seus empregados pelo espaço temporal exigido para cada situação.

O art. 16 da LGPD estipula a necessidade de eliminação dos dados pessoais após as hipóteses de término do tratamento, e autoriza a sua conservação em quatro hipóteses, cabendo destacar no presente estudo a mais relevante para as relações de trabalho, qual seja: o inciso I, que prevê a manutenção dos dados quando necessário for para "*I - cumprimento de obrigação legal ou regulatória pelo controlador*". Referida hipótese se destaca, uma vez que essa norma legitima a guarda dos dados pelo prazo prescricional de cada pretensão associada, em caso de eventual judicialização de um conflito, quando se faz importante, e fundamental inclusive, a produção probatória ampla, composta por documentos e informações, legitimando, assim, o empregador/controlador a guardar os dados até o fim do prazo prescricional.

Merece atenção o fato de que os prazos prescricionais de acordo com o tema nele envolto não são os mesmos. O prazo prescricional trabalhista de 2 (dois) anos (para o ajuizamento da reclamação) conta-se apenas a partir da data de término do contrato de trabalho, porém, os direitos protegidos pela CLT são dos últimos 5 (cinco) anos contados da data da propositura da ação (art. 7º, XXIX, da CF/88), sendo recomendável não se descuidar desse importante fator. Prescrições distintas também devem ser mapeadas, tais como as das doenças ocupacionais, que podem se manifestar apenas depois de determinado lapso temporal e que têm o início de contagem do prazo prescricional apenas com a sua ciência inequívoca (Súmula 230 do STF e Súmula 278 do STJ), o que pode ocorrer muito tempo depois de rescindido o contrato. Há hipóteses, ainda, de ações em que permeiam o debate sobre a existência ou inexistência de vínculo de emprego, que são imprescritíveis segundo o artigo 11 da CLT.

Diante desse contexto, destaca-se que o ideal é não se limitar ao prazo literal de prescrição, sendo possível a guarda mais prolongada ou até mesmo indeterminada em relação à documentos essenciais para se defender de pretensões imprescritíveis.

5 O POLÊMICO CONSENTIMENTO DADO PELO EMPREGADO PARA TRATAR DADOS NO CONTRATO DE TRABALHO É VÁLIDO? É ARRISCADO?

A primeira hipótese que viabiliza ao controlador/empregador o tratamento de dados pessoais é o "fornecimento de consentimento pelo titular", presente no artigo 7º, inciso I da LGPD. No entanto, o art. 8º, § 2º, do mesmo diploma legal aponta ser responsabilidade deste controlador o ônus de provar que o consentimento se deu de forma lícita. Logo, utilizar o termo de consentimento como justificativa central para o tratamento de todos os dados pessoais de empregados no curso da relação de emprego poderá ensejar riscos ao empregador.

Isto se apresenta, pois retroagindo ao art. 5º, inciso XII, da LGPD, deparamo-nos com o conceito de "consentimento" à luz dos vetores dessa lei, que deve ser entendido como a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[20].

Nesse sentido, considerando serem as leis trabalhistas protetivas do empregado em sua gênese, no afã de amparar o hipossuficiente da relação, logo se questiona se a expressão "manifestação livre" da vontade estaria verdadeiramente presente no âmbito de uma relação de labor, que é marcada naturalmente por um desequilíbrio de poder, subordinação e, em regra, pela dependência econômica, que poderá levar o trabalhador a uma esfera de ausência de opção. Daí a importância de reflexão sobre o tripé FAN, da necessidade x adequação x finalidade, na proteção de

---

[20] "Art. 5º Para os fins desta Lei, considera-se:
(...)
XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada." Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados. Brasília. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 abr. 2023.

dados pessoais de empregados, para afastar-se ao máximo das situações que exijam tal elemento.

Assim, não é difícil concluir que a generalização e a informação vaga do dispositivo legal concernente ao consentimento exigirão adequação na esfera do Direito do Trabalho face a essas singularidades e tipicidades. Além disso, esse consentimento ganha maior equilíbrio quando se está no campo dos dados do hiperssuficiente, que é aquele descrito por lei como sendo o portador de condições diferenciadas que lhe guindam à possibilidade de transacionar e até de renunciar à direitos, dadas suas condições diferenciadas de escolaridade e de remuneração[21]

De qualquer modo, também não se afigura correto ter como premissa que referido consentimento jamais poderá ser isento de interferências e dependências do empregado para com seu empregador, inutilizando-o na esfera laboral, mormente quando se está diante de um trabalhador, por exemplo, com poderes de gestão. Inúmeras são as hipóteses de dados e seu tratamento, quando então, caso a caso, o consentimento deve ser sopesado em conjunto com os princípios que regem a LGPD, adaptados às circunstâncias das relações de emprego.

6 AFINAL, QUAIS DADOS PESSOAIS PODEM SER TRATADOS DIANTE DE DIVERSAS REALIDADES PRESENTES NAS RELAÇÕES EMPREGATÍCIAS?

Considerando as diversas realidades das relações empregatícias, não há como elencar especificamente quais dados podem ser tratados sem a análise de caso a caso, usando sempre as imposições legais de hipóteses e os princípios como premissas estruturantes do "edifício-jurídico", que orientam com clareza explicativa a subsunção dos fatos na norma. Os dados pessoais, sensíveis ou não, estarão associados a determinados contextos que serão capazes, ou não, em tese, de gerar uma violação.

Desta forma, acredita-se que a relação de emprego é uma das áreas em que há maior volume de tratamento de dados pessoais, inclusive de dados pessoais

---

[21] Parágrafo único do artigo 444 da CLT c/c artigos 611-A e 611-B da CLT. (BRASIL. **Consolidação das Leis do Trabalho (1943)**. Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 30 abr. 2023).

sensíveis, tais como os dados de saúde, filiação a sindicato, dados biométricos e tantos outros acima elencados. Então, caberá ao controlador identificar cuidadosamente as bases legais que autorizam o tratamento e, havendo mais de uma hipótese, ancorar-se naquela que seja mais segura e específica. Isso, porque, conforme apontado nos princípios da LGPD, o tratamento de dados pessoais deve ser adequado, limitado ao estritamente necessário e restrito à finalidade legitimadora específica.

7 QUAL A RESPONSABILIDADE DA FIGURA DO OPERADOR DE DADOS DIANTE DA CONDIÇÃO DE EMPREGADO?

A definição concisa das funções/papéis do controlador e do operador dos dados constam respectivamente nos incisos VI e VII do art. 5º da LGPD. O primeiro (controlador) é, no texto legal, a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais", ou seja, é em síntese aquele que detém o domínio dos fatos e dados a serem tratados, portanto, por eles responsável. Detalhe que aqui merece relevo, ocorre quando o controlador compartilha os dados coletados das relações de trabalho com terceiros, como, por exemplo, com escritórios de contabilidade que realizam a folha de pagamento dos empregados e, nesse caso, o gestor da folha também se tornará controlador. Já o segundo (operador), conforme texto do artigo citado, é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador", ou seja, aquele que processa os dados em nome do controlador r e conforme a finalidade por este delimitada. Então, a principal diferença entre o controlador e operador é o poder de decisão, porque o operador só pode agir no limite das finalidades determinadas pelo controlador.

Aplicar essas definições na esfera das relações de trabalho de forma genérica coloca o empregador, via de regra, na função de controlador, e a tarefa do operador (que poderá, ou não, existir) a ser assumida por um empregado que, em nome do empregador, realizará o tratamento de dados pessoais. Essa prática não é recomendada porque a Autoridade Nacional de Proteção de Dados (ANPD) brasileira

editou, em maio de 2021, o "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado", no qual ficou registrado o entendimento de que empregados, administradores, sócios, servidores e outras pessoas naturais que integram a pessoa jurídica e cujos atos expressam a atuação desta, não devem ser considerados operadores, tendo em vista que o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos.[22]

Especificamente nessa hipótese em que o empregado é também, o operador, embora esteja ligado ao controlador por uma relação de emprego, e subordinada por lei, ainda assim, sua responsabilidade será solidária pelos danos causados pelo tratamento, se descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador (patrão), hipótese em que o operador equipara-se ao controlador, a teor do art. 42, § 1º, I, da LGPD. Logo, a relação de emprego por si só, não impedirá o empregado de ter que indenizar danos, caso aceite o encargo de operador, e não observe as instruções do controlador e sobretudo da Lei Geral de Proteção de Dados.

8 COMPLIANCE TRABALHISTA COMO ALTERNATIVA ÀS BOAS PRÁTICAS NA PROTEÇÃO DE DADOS PESSOAIS DOS EMPREGADOS

Em breves assertivas destaca-se que caberá aos controladores e/ou operadores de dados empenharem-se na busca de métodos que auxiliem no uso responsável dos dados. Essa realidade assenta-se, pois, a LGPD impõe genericamente a adoção de medidas de segurança, nos termos do artigo 46, e a faculdade de formulação de regras de boas práticas e de governança, nos termos do artigo 50 e seguinte do mesmo diploma. Por isso, acredita-se que a bandeira do *compliance*[23] é levantada para alcançar não apenas o cumprimento de lei, mas

---

[22] Item 58 do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. Disponível em: https://www.gov.br/anpd/pt-br/documentosAgentesdeTratamento_Final.pdf. Acesso em: 7/9/2023.
[23] O Compliance relacionado à seara laboral, além de estar em consonância com a função social e a responsabilidade socioambiental da empresa, agregam valor à entidade empresarial e atrai consumidores, investidores e parceiros, proporcionando um aumento significativo do lucro. (MARCOLINO, Beatriz Aparecida; SILVEIRA, Daniel Barile da. A Lei Geral De Proteção De Dados E As

também para regulamentar um arsenal de condutas que devem ser disciplinadas para que, com estratégias, o objetivo seja atingido.

Proveitoso dizer ainda que, diante de eventual demanda judicial, pode o magistrado inverter o ônus da prova, nos termos do artigo 42, §2º da Lei Geral de Proteção de Dados, coadunando com o artigo 818, §1º da Consolidação das Leis do Trabalho. A inversão citada tem respaldo legal, na medida em que em âmbito trabalhista a vulnerabilidade do trabalhador é presumida, e não seria diferente no momento da comprovação de alegação de prejuízo pelo tratamento de dados equivocadamente.

Assim, por fim acredita-se que a prevenção sob todos os aspectos deve ser priorizada, uma vez que pode compensar tanto em âmbito financeiro para as empresas e/ou empregadores – pois a punição tem aptidão para alcançar colossal sanção pecuniária e as demandas das reclamações trabalhistas tendem a crescer – , como em outros aspectos, tais como a própria imagem do estabelecimento.

CONSIDERAÇÕES FINAIS

A coleta de dados pessoais nas relações de trabalho, especialmente no contexto digital, realmente levanta várias preocupações de privacidade e segurança. Algumas das principais preocupações incluem a privacidade dos funcionários, já que a coleta excessiva ou desnecessária de dados pessoais pode incluir informações/dados sensíveis, como estado de saúde, orientação sexual, filiação sindical e outras informações pessoais que nem sempre serão pertinentes para a relação de trabalho.

Desta forma, afastar-se do uso indevido dos dados também é fator relevante, evitando-se monitorar ou controlar os funcionários para tomada de decisões futuras e discriminatórias ou com invasão da vida pessoal dos trabalhadores. A falta de transparência sobre como os dados serão coletados, processados e usados pode igualmente resultar em uma falta de consentimento informado dos funcionários, violando a Lei Geral de Proteção de Dados.

Relações De Trabalho: O Compliance Como Alternativa. **Revista Juris UniToledo**, Araçatuba, SP, v. 05, n. 04, p. 206-224, out./dez., 2020).

Todas as possibilidades de coleta de dados de personalidade, padrões e informações podem, por um lado, desencadear ações benéficas ao mercado de trabalho, mas, por outro lado podem gerar condutas preconceituosas, segregadoras e exclusivas, o que nos exige uma reflexão acerca da importância do sigilo, da intimidade, privacidade e sobretudo da proteção dos dados pessoais que são coletados no ambiente laboral.

Poucas pesquisas abertas existem sobre a efetiva utilização de algoritmos em banco de dados de colaboradores e o quanto essa automação é fator relevante ou decisivo no tocante às novas contratações, aferimento de produtividade, percepção de prêmios, promoções ou até demissões, e menos ainda sabe-se se, de fato, esses dados têm sido convertidos em decisões assertivas para os negócios e para os envolvidos. Contudo, o fato é que não há proibição ao tratamento de dados, ao contrário, a Lei 13.709/18 deu ao titular dos dados o empoderamento deles e o direito de autodeterminação informativa, e regulamentou o legítimo exercício prevendo punições administrativas para os casos de ilicitude.

Sobre o tema, importante referir que é necessário adotar as políticas de segurança e de boas práticas para a governança de dados dos funcionários com o intuito de não os deixarem em uma posição de vulnerabilidade, inclusive para evitar passivos trabalhistas perante a Justiça do Trabalho e fiscalizações dos órgãos reguladores. Nesse sentido, nos ensina Regina Ruaro[24], professora e pesquisadora:

> Dificilmente um operador do direito, ao analisar os problemas relacionados à era digital, não se depara com situações paradoxais e conflitantes. Assim também ocorre ao se tratar do tema de proteção de dados pessoais, na medida em que, fruto do direito à privacidade, extrapola seus limites, comunicando-se livremente com conceitos e vocábulos metajurídicos. Inicialmente, está contido no âmbito da privacidade, mas o supera, abarca e re-significa, funcionando como livre espaço de mediação.[25].

---

[24] RUARO, Regina Linden; RODRIGUEZ Daniel Piñeiro; FINGER Brunize. O Direito à proteção de dados pessoais e a privacidade. **Revista da Faculdade de Direito** - UFPR, Curitiba, n.47, p.29-64, 2008.

[25] DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law** [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 6 set. 2023, p. 403.

Sendo assim, diante de um cenário de crescente digitalização e interconectividade, a complexa *interplay* entre a coleta necessária de informações e o respeito à autonomia dos trabalhadores impõe uma abordagem cautelosa e equilibrada. Nesse contexto, acredita-se que a implementação eficaz de regulamentações adequadas e a promoção de uma cultura de conscientização são cruciais para assegurar um ambiente laboral onde a inovação coexista harmoniosamente com a salvaguarda dos direitos fundamentais.

REFERÊNCIAS

ALCASSA, Flávia. A Lei Geral de Proteção de Dados Pessoais (LGPD) E A Exposição de Dados Sensíveis Nas Relações de Trabalho. **Revista Síntese**: Trabalhista e Previdenciária. Rev. do Trib. Reg. Trab. 10ª Região, Brasília, v. 24, n. 2, p. 145-51, 2020.

______________ O papel da Lei Geral de Proteção de Dados Pessoais (LGPD) nas relações de trabalho. **Revista Síntese**: Trabalhista e Previdenciária, v. 31, n. 375, p. 58-65, set. 2020.

ALCASSA, Flávia; CASTELANI, Liliana. **Lei Geral de Proteção de Dados Pessoais e o Impacto nas Relações de Emprego**. Associação Nacional dos Profissionais de Privacidade de Dados, 2020.

ALVES, Amauri César; ESTRELA, Catarina Galvão. Consentimento do trabalhador para o tratamento de seus dados pelo empregador: análise da subordinação jurídica, da higidez da manifestação de vontade e da vulnerabilidade do trabalhador no contexto da LGDP. **Revista Síntese**: Trabalhista e Previdenciária, São Paulo, v. 31, n. 375, p. 25-40, set. 2020.

ARAÚJO JÚNIOR, Francisco Milton. **Parâmetros Para Delimitação Do Meio Ambiente Do Trabalho Na Volatividade Da Sociedade Contemporânea (Ciberespaço)**. *In*: FELICIANO, Guilherme Guimarães. Direito ambiental do trabalho: apontamentos para uma teoria geral. São Paulo: LTr, p. 41-47, 2017.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF: Senado, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 03 mai. 2023.

BRASIL. **Consolidação das Leis do Trabalho (1943)**. Consolidação das Leis do Trabalho. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 30 abr. 2023.

BRASIL. **Decreto n. 10.854, de 10 de novembro de 2021**. Regulamenta disposições relativas à legislação trabalhista e institui o Programa Permanente de Consolidação, Simplificação e Desburocratização de Normas Trabalhistas Infralegais e o Prêmio Nacional Trabalhista, e altera o Decreto 9.580, de 22 de novembro de 2018. Brasília, DF: Presidência da República, 2021. Disponível em: https://www.planalto. gov.br/ccivil_03/_ato2019-2022/2021/decreto/d10854.htm. Acesso em: 28 abr. 2023.

BRASIL. **E-ED-RR – 182000-05.2013.5.13.0008**. Relatora Ministra: Maria Cristina Irigoyen Peduzzi, Subseção I Especializada em Dissídios Individuais, 24 mai. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados. Brasília. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 abr. 2023.

BRASIL. Tribunal Superior do Trabalho. **Processo n.TST-AIRR-597-43.2012.5.02.0009**. Recurso de Revista interposto na vigência da Lei 13.015/2014. Custas a cargo do reclamante. Recolhimento pela reclamada ao interpor recurso ordinário. Inversão do ônus da sucumbência. Deserção. Inocorrência. Relatora: Min. Maria Helena Mallmann, 3 set. 2019. Disponível em: https://consultadocumento.tst.jus.br/consultaDocumento/acordao.do?anoProcInt=2015&numProcInt=203616&dtaPublicacaoStr=06/09/2019%2007:00:00&nia=7384236. Acesso em: 28 mai. 2022.

BRASIL. Tribunal Superior do Trabalho. **RR: 2430005820135130023**. Recurso de revista. Processo representativo da controvérsia do incidente de recursos repetitivos - tema nº 1. Exigência de certidão de antecedentes criminais de candidatos a emprego. Indenização por dano moral. Relator: Márcio Eurico Vitral Amaro, 30 mai. 2016.

DONEDA, D. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law** [EJJL], [S. l.], v. 12, n. 2, p. 91–108, 2011. Disponível em: https://periodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 6 set. 2023.

ESOCIAL. O Decreto nº 8373/2014 instituiu o Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas (eSocial). **SPED** (Sistema Público De Escrituração Digital). Disponível em: http://sped.rfb.gov.br/pagina/show/1507#:~:text=O%20Decreto%20n%C2%BA%208373%2F2014,Previdenci%C3%A1rias%20e%20Trabalhistas%20(eSocial). Acesso em 01 mai. 2023.

FINCATO, Denise Pires; BITENCOURT, Manoela de. Ciber como Local de Trabalho: o problema (ou a solução?) do teletrabalho transnacional. **Quaestio Iuris**, Rio de Janeiro, v. 08, n. 04, p. 2237-2263, 2015.

FINCATO, Denise Pires; FRANK, Marina Silveira. Bring Your Own Device (BYOD) e suas Implicações nas Relações de Emprego: reflexões práticas. **Revista Magister de Direito do Trabalho**, São Paulo, v. 15, n. 89, p. 17-35, mar./abr. 2019.

GULARTE, Caroline de Melo Lima. **A Proteção de Dados Pessoais no Uso de Tecnologia na Relação de Emprego**: efeitos do compliance trabalhista digital nas negociações coletivas. Dissertação (Programa de pós-graduação em Direito) – PUCRS, 2020. Disponível em: https://tede2.pucrs.br/tede2/handle/tede/9306. Acesso em: 6 set. 2023.

JUNIOR, Carlos Augusto Pinto de Vasconcellos; FERREIRA, Victor Silva. Impacto Da Lei Geral De Proteção De Dados Pessoais Nas Relações De Trabalho: a necessidade de implantação do programa de integridade (Compliance). **UERJ Labuta**. 21 de março de 2020. Disponível em: https://uerjlabuta.com/2020/03/21/impacto-da-lei-geral-de-protecao-de-dados-pessoais-nas-relacoes-detrabalho-a-necessidade-de-implantacao-do-programa-de-integridade-Compliance/. Acesso em: 20 abr. 2023.

MECANISMOS de pesquisa que permitem acesso à ações criminais e trabalhistas a partir da consulta de dados pessoais viola LGPD, entenda. **IAPP** (International Association of Privacy Professionals). Disponível em: https://www.lgpdbrasil.com.br/mecanismos-de-pesquisa-que-permitem-acesso-a-acoes-criminais-e-trabalhistas-a-partir-da-consulta-de-dados-pessoais-viola-lgpd-entenda/. Acesso em: 2 mai. 2023.

MALLET, Estevão. **Apontamentos Sobre A Competência Da Justiça Do Trabalho Após E Emenda Constitucional N. 45**. In: Direito, Trabalho e Processo em Transformação. São Paulo, LTR, 2005.

MARCOLINO, Beatriz Aparecida; SILVEIRA, Daniel Barile da. A Lei Geral De Proteção De Dados E As Relações De Trabalho: O Compliance Como Alternativa. **Revista Juris UniToledo**, Araçatuba, SP, v. 05, n. 04, p. 206-224, out./dez., 2020.

MARCONDES, Rui Jose Leite Santana. A lei geral de proteção de dados à luz dos instrumentos coletivos de trabalho (CCT e ACT) que impõem o fornecimento de dados. **Rev. Trib. Trab. 2. Reg.**, São Paulo, v. 14, n. 28, p. 120-134, jul./dez. 2022.

MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. **As Bases Legais de Tratamento de Dados no Ambiente de Trabalho**: Análise da Adequação Entre a LGPD e a Lei Trabalhista. *In*: MIZIARA, Raphael; MOLLICONE, Bianca; PESSOA, André. Reflexos da LGPD no Direito e no Processo do Trabalho. São Paulo (SP): Editora Revista dos Tribunais. 2022. Ebook, Disponível em: https://www.jusbrasil.com.br/doutrina/reflexos-da-lgpd-no-direito-e-no-processo-do-trabalho/1590440816. Acesso em: 1 mai. 2023.

PORTARIA SEPRT nº 1127 de 14/10/2019. Define as datas e condições em que as obrigações de prestação de informações pelo empregador nos sistemas CAGED e

RAIS serão substituídas pelo Sistema de Escrituração Digital das Obrigações Fiscais, Previdenciárias e Trabalhistas - eSocial. (Processo nº 19965.103323/2019-01). **LEGISWEB**. 2019. Disponível em: https://www.legisweb.com.br/legislacao/?id=383471. Acesso em: 01 mai. 2023.

ROMAR, Carla Teresa Martins. **Direito do Trabalho Esquematizado**. São Paulo, Editora Saraiva, 5.ª ed., 2018.

RUARO, Regina Linden; HAINZENREDER JUNIOR, Eugênio. **Proteção da privacidade no contrato de trabalho: da normatização legal a situações de conflitos.** Espaço Jurídico Journal of Law, Joaçaba, v.16, n. 2, p. 601-634, 2015.

RUARO, Regina Linden; RODRIGUEZ Daniel Piñeiro; FINGER Brunize. O Direito à proteção de dados pessoais e a privacidade**. Revista da Faculdade de Direito - UFPR**, Curitiba, n.47, p.29-64, 2008.

SANDEN, Ana Francisca Moreira de Souza. **A proteção de dados pessoais do empregado no direito brasileiro**: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado. Tese (Doutorado em Direito do Trabalho) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2012. Disponível em: https://teses.usp.br/teses/disponiveis/2/2138/tde-05082013-165006/pt-br.php. Acesso em: 26 abr. 2023.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel Francisco. **Curso de direito constitucional**. 7. ed. rev., atual. e ampl. São Paulo: Saraiva, 2018.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Luxembourg: EUR-Lex, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 02 mai. de 2023.

UNIÃO EUROPEIA. **General Data Protection Regulation – GDPR**. Disponível em: https://gdpr-info.eu/. Acesso em 04 jun. de 2023.

6. OBSTÁCULOS À PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

https://doi.org/10.36592/9786554600712-06

Kim William Pinto Mendonça[1]

RESUMO

O presente artigo abordará a sociedade da informação e os obstáculos relacionados à privacidade no contexto atual. Para tanto, será considerado o rápido avanço tecnológico e a crescente quantidade de dados pessoais disponíveis e utilizados, com e sem o consentimento dos usuários, tornando a proteção da privacidade um desafio cada dia mais complexo. O objetivo deste estudo será a análise dos principais obstáculos atualmente enfrentados na sociedade da informação e discussão das medidas legais e regulatórias necessárias para proteção da privacidade dos indivíduos.
Palavras-chave: Sociedade da informação. Privacidade. Desafios.

PRIVACIDADE E PROTEÇÃO DE DADOS NA SOCIEDADE ATUAL

BREVE HISTÓRICO: A SOCIEDADE DA INFORMAÇÃO

A sociedade pós-industrial, caracterizada pelas transformações decorrentes do desenvolvimento e expansão da indústria, propiciaram um ambiente favorável para o progresso de novas tecnologias.

> A expressão "sociedade da informação" passou a ser utilizada, nos últimos anos desse século, como substituto para o conceito complexo de "sociedade pós-industrial" e como forma de transmitir o conteúdo específico do "novo paradigma técnico-econômico[2].

---

[1] Mestrando Pontifícia Universidade Católica do Rio Grande do Sul - PUCRS. Área de Concentração: Fundamentos Constitucionais do Direito Público e do Direito Privado. Linha de Pesquisa: Eficácia e Efetividade da Constituição e dos Direitos Fundamentais no Direito Público e Direito Privado. Bolsista CAPES – TAXA. Advogado.

[2] WERTHEIN, Jorge. A Sociedade da Informação e seus desafios. Disponível em:[<https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt> Acesso em 07 agosto 2023.

Assim, a relevância cada vez maior da informação em nossa sociedade é discutida com seriedade por sociólogos há, pelo menos, trinta anos, período em que da teoria à prática, já ocorreram transformações tecnológicas que sequer poderiam ter sido imaginadas, a exemplo das razões para as quais a internet foi desenvolvida, no contexto da Guerra Fria[3], e a forma de utilização e o alcance atual.

Conforme o livro “A Sociedade em Rede” do sociólogo Manuel Castells[4]:

> Sem dúvida, a habilidade ou inabilidade de as sociedades dominarem a tecnologia e, em especial, aquelas tecnologias que são estrategicamente decisivas em cada período histórico, traça seu destino a ponto de podermos dizer que, embora não determine a evolução histórica e a transformação social, a tecnologia (ou sua falta) incorpora a capacidade de transformação das sociedades, bem como os usos que as sociedades, sempre em um processo conflituoso, decidem dar ao seu potencial tecnológico.

Logo, para além das finalidades visadas é inequívoco que as transformações decorrentes da sociedade da informação, bem como a interconectividade dos dados tem por um lado impactado (e facilitado) muito a vida em sociedade, mas por outro aumentado de forma exponencial o risco de invasão da privacidade, o que será, neste artigo, explorado observando situações pontuais.

Pois bem. É inequívoco que a internet alcançou os mais diversos espaços da vida em sociedade, fazendo com que estejam abarcados praticamente todos os aspectos no mundo virtual.

Isto é, os sistemas desenvolvidos permitem que em apenas alguns cliques estejam salvas fotografias, senhas e sejam lembrados compromissos assumidos a qualquer momento em qualquer lugar. Mais. É possível que sejam enviadas e

---

[3] Após o lançamento do primeiro satélite Sputnik pelos soviéticos em 1957, ultrapassando os Estados Unidos da América (EUA) na corrida pelo espaço, o Departamento de Defesa dos Estados Unidos afim de acelerar o progresso tecnológico criou o Advanced Research Projects Agency (ARPA). Ela foi criada com objetivos estritamente militares e com o intuito de interligar as bases militares americanas. - Internet: do início à era da semântica. Disponível em: <https://biblioteca.univap.br/dados/00003d/00003da9.pdf>. Acesso em 07 agosto de 2023.

[4] CASTELLS, Manuel. A Sociedade em Rede. Volume I. 8 edição. Disponível em: <https://perguntasaopo.files.wordpress.com/2011/02/castells_1999_parte1_cap1.pdf> Acesso em 07 de agosto de 2023.

recebidas mensagens de forma instantânea e que as pessoas façam-se presentes de modo virtual e concomitantemente em compromissos geograficamente distantes, questões que facilitam em muito o dia a dia das pessoas em uma sociedade reconhecida pela falta de tempo.

> Os serviços estão sendo acessados por pessoas com os mais diferentes conhecimentos e devem atender de forma eficiente a todos eles. Monitoramentos são realizados constantemente baseados em ações dos usuários e a partir destes estudos são realizadas alterações e melhorias nos sistemas. A grande massa de usuários e sua participação efetiva colaboram para este tipo de melhoria[5].

Contudo, para todo e qualquer acesso são necessários que dados pessoais e, por vezes, até mesmo considerados sensíveis sejam fornecidos a provedores e servidores que possibilitam o acesso e utilização de tais sistemas.

Por óbvio que todo desenvolvedor possui em seus programas mecanismos de proteção. Entretanto, verifica-se que a grande maioria (e porque não dizer a totalidade) estão suscetíveis a vazamentos de dados através de ataques por profissionais conhecidos como *"hackers"*, bem como pelo uso indevido por parte da própria empresa que pode utilizar as informações que possui com finalidade comercial, ou ainda, compartilhar com determinado país caso a fundamentação do pedido seja adequada (ainda que seja genérica, como por exemplo, segurança nacional).

> A maioria dos profissionais de tecnologia, em algum momento, já se deparou com problemas relacionados à utilização de seus sistemas que não foram considerados na fase de projeto, ou que foram ao menos, subestimados pelos projetistas. Uma vez que o comportamento humano é complexo e envolve variáveis que não podem ser controladas, se torna difícil, para profissionais da informação, pensar no usuário humano como um componente dos sistemas com que trabalham e que abrangem não apenas máquinas e métodos organizados

---

[5] LIMA, Francisco Rodolfo Vilela. Internet: do início a era semântica Disponível em: <https://biblioteca.univap.br/dados/00003d/00003da9.pdf>. Acesso em 07 agosto de 2023.

> para coletar, processar, transmitir e disseminar dados que representam informação para o usuário. Assim, parece bem mais confortável aderir às variáveis que podem, de fato, ser controladas, tais como *hardware* e *software*[6].

Conclui-se, assim, que um dos maiores obstáculos relacionados à garantia da privacidade na sociedade atual é a coleta excessiva e indiscriminada de dados pessoais por organizações que, na maioria das vezes, sequer se tem conhecimento de onde estão devidamente sediadas, com registro formal em locais longínquos e estrangeiros, não sendo possível afirmar que não obstante a existência da proteção formal, por determinado ordenamento jurídico, seja garantida a proteção necessária e prevista em lei em relação aos dados dos usuários.

Isto porque, os denominados *"cookies"*[7] são ferramentas desenvolvidas para armazenagem de dados que fazem com que as empresas tenham uma significativa quantidade de informações sobre os indivíduos, que vão desde dados básicos, como nome e endereço, até informações mais pessoais, como *hobbies*, interesses de consumo, de saúde, preferência sexual, localização geográfica, fotografias dentre outras.

> De acordo com Siebecker (2003, p. 893-6), o problema clássico em relação ao *cookie* diz respeito ao seu depósito pelo site sem a devida autorização do usuário e seu emprego na coleta e manutenção de informações pessoais, revelando padrões de acesso, preferências e característica. Ele cita o caso da empresa DoubleClick Inc., pertencente à Google, responsável pela oferta de mais de 60 bilhões de anúncios mensais na rede, cuidadosamente interligados a perfis de mais de 100 milhões de usuários rastreados online[8].

---

[6] PILAR DA SILVA, Denise Ranghetti; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. Ciênc. cogn., Rio de Janeiro, v. 10, p. 46-53, mar. 2007. Disponível em: <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1806-58212007000100006&lng=pt&nrm=iso> acessos em 07 ago. 2023.

[7] Como explica Lessig (2006, pp. 07; 48), os cookies de navegador foram ferramentas imprescindíveis para o desenvolvimento da Internet, sobretudo em seu ajuste para comportar o comércio virtual. OLIVEIRA, J. V; SILVA, L. A. "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/download/8419/6309>. Acesso em: 07 ago. 2023.

[8] OLIVEIRA, J. V; SILVA, L. A. "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/download/8419/6309>. Acesso em: 07 ago. 2023.

Situação ainda mais grave se verifica quando se volta a um passado recente, no qual os dados eram coletados e armazenados sem ciência ou consentimento do usuário, gerando preocupações sobre como essas informações poderiam ser utilizadas ou mesmo compartilhadas já que antes da edição da Lei Geral de Proteção de Dados, datada de 14 de agosto de 2018, a previsão legal de privacidade e proteção de dados era limitada.

Outrossim, a dificuldade de fiscalização em razão da regulamentação tardia apresenta outro grande problema: a falta de transparência por parte das empresas e governos em relação ao armazenamento e uso das informações. Os termos e condições de uso são textos extensos e considerados complexos para o usuário que não possui conhecimento técnico sobre o tema, dificultando a compreensão sobre o uso dos dados.

> A comunidade de segurança da informação recentemente deu-se conta de que o comportamento do usuário desempenha um papel importante em incidentes de segurança. Sistemas de segurança da informação são frequentemente comparados a uma corrente com muitos elos representando os componentes envolvidos, tais como equipamento, *software*, protocolos de comunicação de dados, e outros, incluindo o usuário humano. Na literatura sobre segurança da informação, o usuário humano é frequentemente referenciado como o elo mais fraco (Sasse *et al.*, 2001)[9].

A grande assimetria na relação entre o usuário e as empresas, decorrente da hipossuficiência informacional, possibilita que se consiga até mesmo ocultar as reais intenções ou efetivo uso destas informações.

> O que os resultados de Ayenson e outros demonstram é que as tecnologias verificadas nos *cookies* possuem uma capacidade de disseminação e de operação que extrapolam as habilidades de usuários comuns da Internet. Assim, mesmo que o usuário opte por controlar os *cookies* de seu próprio navegador, é

[9] PILAR DA SILVA, Denise Ranghetti; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. Ciênc. cogn., Rio de Janeiro, v. 10, p. 46-53, mar. 2007. Disponível em <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1806-58212007000100006&lng=pt&nrm=iso> acessos em 07 ago. 2023.

> possível que ele não consiga lidar com certas estratégias de armazenamento e de coleta de dados pessoais na rede e permaneça incessantemente monitorado no plano virtual[10].

Ademais, há também que se atentar a uma possível vigilância em massa. Isto é, Estados, através de suas agências de segurança estão implementando programas extensivos de monitoramento digital, com vigilância por câmeras inteligentes que captam imagens de todas as cidades, vigilância nas telecomunicações, nas transações financeiras, coleta de metadados, dentre outros.

Denota-se que tais medidas são comumente justificadas como necessárias para a proteção da segurança nacional, ou combate à criminalidade, mas não deixam de suscitar dúvidas sobre a real imprescindibilidade de captação e sobre a forma que garantirá a proteção da privacidade dos indivíduos.

Portanto, os problemas envolvendo a privacidade na sociedade da informação são complexos e afetam praticamente todas as áreas da vida em sociedade. A coleta excessiva de dados, a falta de transparência, a vigilância em massa, o compartilhamento indiscriminado de informações são apenas alguns exemplos à ameaça que a privacidade enfrenta em nossa sociedade.

É, pois, essencial que haja uma reflexão aprofundada sobre o tema, a fim de buscar meios que levem a uma convivência pacífica garantindo os avanços tecnológicos sem descuidar do respeito e da efetivação do direito fundamental à privacidade dos indivíduos.

PRIVACIDADE: O ENFOQUE DO DIREITO CONSTITUCIONAL

A Constituição de 1988, elencou no rol previsto no artigo 5º, dentre os direitos fundamentais, para proteção da dignidade e da personalidade humana, o direito à privacidade, o qual é um dos mais relevantes.

---

[10] OLIVEIRA, J. V; SILVA, L. A. "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/download/8419/6309>. Acesso em: 07 ago. 2023.

Ainda, a importância e base do direito é mais antiga, sendo possível extrair da leitura de dispositivos que se encontram, por exemplo, na Declaração Universal dos Direitos do Homem, de 1948[11].

“Artigo 12: Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.”

O direito à privacidade engloba diversas questões importantes, que perpassam pontos sensíveis aos indivíduos, desde poder ter uma vida sem a ingerência do Estado sobre aspectos pessoais até ter a sua autonomia protegida de terceiros, respeitadas as informações que, a priori, dizem respeito apenas a si.

Dessa forma, conforme lecionou Sarlet,

> Nessa perspectiva, é crucial que se tenha presente que, embora a proteção de dados tenha sido deduzida (associada), em diversos casos, do direito à privacidade (v.g., nos EUA, o conceito de informational privacy) ou, pelo menos, também do direito à privacidade, como no caso da Convenção Europeia de Direitos Humanos (nos termos da exegese do art. 8º levada a efeito pela CEDH), o fato é que o objeto (âmbito de proteção) do direito à proteção de dados pessoais é mais amplo, porquanto, com base num conceito ampliado de informação, abarca todos os dados que dizem respeito a determinada pessoa natural, sendo irrelevante à qual esfera da vida pessoal se referem (íntima, privada, familiar, social), descabida qualquer tentativa de delimitação temática[12].

Portanto, era sentida a inexistência, até pouco tempo, da expressa previsão da proteção dos dados pessoais, o que se efetivou com a Emenda Constitucional 115 de 2022, acrescentando-se o inciso LXXIX ao art. 5º da Constituição Federal[13]:

“LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.”

---

[11]Declaração Universal dos Direitos do Homem. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos> Acesso 08 ago. 2023.
[12] SARLET, Ingo. Direitos Fundamentais & Justiça | Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020
[13]____BRASIL. Constituição Federal de 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso 11 de ago. 2023.

TÓPICOS IMPORTANTES PARA ENTENDER A PRIVACIDADE

TEORIA DOS CÍRCULOS CONCÊNTRICOS

A classificação realizada por Heinrich Hubmann, aqui sintetizada, de acordo com as ideias compiladas em artigo apresentado e debatido no XXV Encontro Nacional do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI)[14], dividiu a vida privada em três círculos concêntricos, quais sejam: esfera íntima (*Intimisphare*), voltada à vida privada de cada indivíduo; esfera secreta (*Geheimnisphare*), compreendendo pessoas que possuem relação com a vida íntima; e, esfera privada (*Privatsphare*), que por ser mais ampla permite desenvolver a personalidade.

No entanto, conforme esclarece Doneda [15] , a teoria supracitada foi abandonada pelo Tribunal Constitucional Alemão, em função da grande subjetividade existente entre os limites de cada círculo. Porém, verifica-se que, no Brasil, é eventualmente utilizada, o que se extrai de julgado do Supremo Tribunal Federal, ainda que com algumas diferenças.

É possível, por exemplo, constatar no acórdão ARE 867326 RG/SC, conforme voto do Relator, no caso, Ministro Paulo de Tarso Sanseverino[16]:

> Tradicionalmente, na jurisprudência alemã, a proteção da vida privada era analisada na perspectiva de três graus ou esferas distintas: intimidade, privacidade e publicidade.
>
> A publicidade é a área de atuação pública de cada pessoa, exposta ao interesse público em geral, e que, consequentemente, apresenta livre atuação pelos meios de comunicação em geral.

[14] PAIVA, Olívia Caetano Salgado. O Direito à Intimidade nas Relações Conjugais Versus Contratualização do Casamento. Direito de família e sucessões I [Recurso eletrônico on-line] organização CONPEDI/UNICURITIBA; Coordenadores: Sergio Pereira Braga, Tereza Cristina Monteiro Mafra, Valéria Silva Galdino Cardin – Florianópolis: CONPEDI, 2016.

[15] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Disponível em <https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais> Acesso 09 ago. 2023.

[16] Recurso Extraordinário. Disponível em: <https://portal.stf.jus.br/jurisprudenciaRepercussao/verPronunciamento.asp?pronunciamento=5567953>. Acesso 09 ago. 2023.

> A privacidade é uma esfera intermediária, cuja proteção é inversamente proporcional ao estatuto social da pessoa; assim, quanto mais pública a pessoa, menor o grau de proteção.
> A intimidade é o último e inviolável reduto da liberdade pessoal, que não pode ser devassada por mais pública que seja a pessoa.
> Esses graus de proteção da vida privada serviram de referência para a doutrina e para a jurisprudência alemã estabelecerem os limites da liberdade de imprensa (...).

O Tribunal Constitucional Alemão, na mesma decisão que entendeu como superada a teoria dos círculos concêntricos, elaborou conceito que, posteriormente veio a ser trabalhado por Rodotà, qual seja, o da autodeterminação informativa: a pessoa deve poder determinar como serão utilizadas as suas informações, isto é, de forma a impedir ou limitar o seu uso quando pertinente.

A MUTABILIDADE E ELASTICIDADE DA PRIVACIDADE

O significado e a maior atenção à privacidade foi modificando com a evolução e o desenvolvimento da sociedade e da mídia[17], como se vê em razão da forma que se apresenta hoje a imprensa, livros, fotografias, computadores, internet, de modo que não há como prever qual será a interpretação a ser aplicada à privacidade daqui a alguns anos, podendo-se afirmar que continuará em constante evolução.

Nesse sentido, tem-se que a última e mais marcante evolução ocorreu segundo Castells[18], na era da informação e ainda, segundo Zuboff[19] no capitalismo

---

[17] Considerando a massificação das novas tecnologias de informação e comunicação, e o ritmo acelerado em que informações podem ser transmitidas, principalmente pela internet, houve uma tendência mundial de que as pessoas passassem a desenvolver uma consciência coletiva sobre privacidade, BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel. A Coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral De Proteção De Dados. Ano 5 (2019), nº 6, 473-514. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf> Acesso 10 ago. 2023.

[18] CASTELLS, Manuel. A Sociedade em Rede. Volume I. 8 edição. Disponível em: <https://perguntasaopo.files.wordpress.com/2011/02/castells_1999_parte1_cap1.pdf> Acesso em: 07 de agosto de 2023.

[19] ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. Intrínseca, 2021.

de vigilância, em decorrência da utilização de dados pessoais como mercadoria na sociedade atual, atribuindo a eles valor comercial.

Superados os argumentos rasos, entende-se que o maior obstáculo que envolve a questão da privacidade é a ausência de fronteiras nesta era da informação e diferentes legislações protegendo a privacidade ao redor do mundo, de forma que se faz necessário padronizar conceitos mínimos e incentivar todos os países a terem normas adequadas de proteção.

Conforme Danilo Doneda[20], a falta de um conceito central na doutrina brasileira faz com que diversas expressões sejam utilizadas como sinônimo: privacidade, vida privada, intimidade, segredo, sigilo, recato, e isso também ocorre na doutrina estrangeira.

Ainda segundo o autor, mais importante do que a definição do conceito é a definição da área que deverá abrangê-lo, e também que a dificuldade de sua definição não é um mal a ser combatido e sim uma característica de sua natureza, de forma que isso deve ser levado em consideração no momento do estudo.

Na sociedade atual, não há que se falar em preservação da privacidade através do isolamento, já que esta não é mais uma opção. A privacidade agora pode ser percebida como uma expectativa de permanecer em um estado de proteção, sem precisar estar constantemente o perseguindo.

Como atual conceito para privacidade pode ser citado o que definiu Rodotà[21] como sendo o direito de manter o controle sobre suas próprias informações e de determinar as modalidades de construção da própria esfera privada.

Doneda[22] entende ainda que, não possuindo aspecto finalístico, o real interesse na sua tutela é a dignidade da pessoa humana, assim como Messinetti, citado por Doneda, considera a privacidade uma "forma" de tutela da pessoa e não um valor em si.

---

[20] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Disponível em: <https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais> Acesso 09 ago. 2023.

[21] RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Maria Celina Bodin de Moraes (org.). Rio de Janeiro: Renovar, 2008.

[22] DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Disponível em: <https://www.academia.edu/23345535/Da_privacidade_%C3%A0_prote%C3%A7%C3%A3o_de_dados_pessoais> Acesso 09 ago. 2023.

A noção tradicional de privacidade, que se restringia a proteger a intimidade, não se compatibiliza com a complexidade da sociedade atual[23]. Ora, tem-se que o conceito foi ampliado para abranger, também, o controle sobre as informações pessoais, o direito ao acesso e acompanhamento dos dados disponíveis, a autodeterminação informativa, dentre outras formas.

PRINCIPAIS OBSTÁCULOS ENVOLVENDO A PRIVACIDADE

A BANALIZAÇÃO DA COLETA DE DADOS PESSOAIS

A denominada era da informação veio acompanhada de uma coleta constante e generalizada de informações pessoais. É comum, a todos, que sejam solicitados e fornecidos dados, tais como: nome, CPF, endereço, e-mail, fotografia, impressões digitais e padrões do rosto, comumente utilizados desde um cadastro em estabelecimento comercial até acessos mais rígidos.

Ocorre que, a banalização do fornecimento de dados, decorrente da normalização na solicitação, reduz o critério do usuário no momento do fornecimento, fazendo com que não seja analisada de forma crítica a real necessidade dos dados que são solicitados e fornecidos.

De igual forma, aumenta a vulnerabilidade pessoal, uma vez que as informações passam a circular de forma rápida e sem a devida segurança, o que dificulta e até mesmo impossibilita, por vezes, a localização da fonte de um vazamento de dados.

"Não obstante, se um dado é considerado como pessoal, por óbvio que está relacionado à pessoa. Logo, por ter esse caráter personalíssimo, qualquer excesso sobre esse tipo de dado pode pôr em risco a privacidade dos cidadãos[24]."

---

[23] O direito de estar só que regia à privacidade transmuta-se e reaparece com uma faceta vinculada à perspectiva de liberdade positiva, onde o sujeito tem o poder de acesso e controle sobre a circulação de suas informações pessoais. (página 79). PEZZI, Ana Paula Jacobus. A necessidade de proteção dos dados pessoais nos arquivos de consumo: em busca da concretização do direito à privacidade. Disponível em <http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf> Acesso 10 ago. 2023.

[24] BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel. A Coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral De Proteção De Dados. Ano 5 (2019), nº 6, 473-514. Disponível em:

Mais. A popularização de drones e câmeras de reconhecimento, tanto referentes a placas de veículo como facial, fez com que o Estado e empresas privadas passassem a desenvolver projetos mais sofisticados de identificação e localização de pessoas.

Embora não se desconheça os benefícios trazidos com o desenvolvimento e aprimoramento de técnicas, que visam colaborar com o aumento dos níveis de segurança pública, tem-se que, na mesma proporção, passam a ficar disponíveis um número ainda maior de dados pessoais, cujo total pode até mesmo ser indeterminável.

COMPARTILHAMENTO DE DADOS SEM CONSENTIMENTO

Importante ponto para reflexão é o compartilhamento de dados entre empresas e órgãos públicos, sem o devido consentimento do usuário, situação que regularmente se verifica como por exemplo, quando uma loja ou um banco vende o cadastro do usuário para empresas de marketing, construtoras, imobiliárias, empresas de telefonia, fazendo com que o indivíduo seja contatado por empresas que jamais teriam a permissão de acesso à tais informações.

Situação ainda mais grave se verifica pelo fato de ser de difícil comprovação, primeiramente em razão da já citada banalização e da alta circulação de dados e, em segundo lugar, pela quase impossibilidade de comprovar a transferência indevida de dados.

Nessa categoria, ainda, é possível enquadrar o uso inadequado dos dados, que ocorre quando o recebedor não respeita o princípio da finalidade[25], utilizando-os de forma distinta daquela consentida e imaginada pelo usuário.

Verifica-se o uso inadequado dos dados quando, por exemplo, um estabelecimento comercial condiciona a realização do cadastro ao fornecimento de telefone celular e e-mail para realizar compra e, com isso, dá início ao envio de informativos publicitários.

<https://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf> Acesso 10 ago. 2023.

[25] MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014, p. 71.

Logo, constata-se que *"Os indivíduos, que são os verdadeiros titulares de seus dados pessoais, terminam por estar sujeitos à violação de sua privacidade sem ao menos se dar conta disso[26]".*

Outro ponto, é quando páginas de busca solicitam o acesso à localização para prestar determinado serviço e, com base nisso, passam a exibir anúncios comerciais diversos, direcionados, ainda que não haja o compartilhamento das informações pessoais com os anunciantes, o usuário está sofrendo com uso indevido do acesso ao local em que se encontra.

POSSÍVEIS SOLUÇÕES PARA PROTEÇÃO DA PRIVACIDADE NA SOCIEDADE DA INFORMAÇÃO

OBSERVÂNCIA ESTRITA ÀS PREVISÕES LEGAIS

As soluções para o respeito à privacidade na sociedade partem da exigência de consentimento do titular dos dados, sua anuência sobre o que será feito com aquela informação, ou seja, o fornecedor da informação precisa estar de acordo com o uso a que será destinado. Não basta uma boa intenção da empresa, com termos informando que respeitam os dados do usuário, é necessário que efetivamente existam medidas para tanto.

Dessa forma, a Lei Geral de Proteção de Dados, nº 13.708/2018 foi uma importante medida de reforço legal e específico para garantia do consentimento, que já era previsto em outros diplomas legais, como bem retratado por Bioni e Luciano[27]:

> (...) a discussão em torno dos adjetivos do consentimento, e por conseguinte, acerca da sua validade no campo da proteção de dados pessoais não se iniciará com a vigência da LGPD. Leis setoriais (e.g., Código de Defesa do Consumidor,

---

[26] BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel. A Coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral De Proteção De Dados. Ano 5 (2019), nº 6, 473-514. Disponível em: <https://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf> Acesso 10 ago. 2023.

[27] BIONI, Bruno Ricardo. E LUCIANO, Maria. O Consentimento como Processo: Em busca do consentimento válido in Tratado de Proteção de Dados Pessoais. Coord. Laura Schertel Mendes. Danilo Doneda. Ingo Wolfgang Sarlet. Otavio Luiz Rodrigues Jr.

> Marco Civil da Internet), a partir de elementos já bastante adensados da dogmática privada brasileira (boa-fé, transparência, dever de informação, abusividade), já o fizeram. Em particular, é importante observar que a racionalidade do debate está ancorada em princípios que foram repisados na LGPD.

Ressaltam os autores, ainda, que o consentimento está associado à informação como dever de quem está recebendo os dados, assim como a transparência, além de o consentimento ser livre, ou seja, partir espontaneamente do titular dos dados.

> Consentir, no sentido em que a LGPD nos aponta, trata-se de um momento de autodeterminação informativa onde o particular faz a manifestação expressa de sua vontade orientando onde, quando, por quem e com qual finalidade suas informações serão utilizadas. Neste sentido, é notória a busca não mais por um consentimento implícito (onde os indivíduos por meio de determinados comportamentos são levados a uma estante de consentimento – a exemplo disso, temos casos onde os titulares preenchem as lacunas de pop up que constam com extensos contratos em reduzidas letras e que se assinam com um toque), mas sim a um consentimento informado (entendido de forma restrita) como maneira de antecipação de riscos de violação à privacidade e busca por um caráter preventivo[28].

Com o respeito ao princípio da informação, da transparência e liberdade de consentimento é que poderá ocorrer a autodeterminação informativa, ou seja, somente assim o titular dos dados terá real poder sobre a circulação das suas informações.

---

[28] BONNA, Alexandre Pereira; CÃNIZO, Amanda de Moura; CALZAVARA, Giovana Ferreira. Consentimento LGPD: Desafios diante da hipervulnerabilidade do Consumidor. Disponível em <https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231/2527> Acesso 10 ago. 2023.

MECANISMOS DE FISCALIZAÇÃO E RESPONSABILIZAÇÃO

Registra-se que, importante forma de inibição de condutas que violem a privacidade dos usuários é possuir sólidos mecanismos de fiscalização e dura responsabilização para quem os violar. Isto é, somente havendo possibilidade de identificar e punir os responsáveis por cuidar dos dados é que haverá engajamento em proteger os dados dos usuários.

Um vazamento de dados pode causar severos danos extrapatrimoniais aos titulares, mas os critérios de estabelecimento de sanções ainda são um tanto quanto subjetivos, isso quando os prejuízos são reconhecidos, sendo preciso que a doutrina e a jurisprudência preencham este espaço deixado pelo legislador.

Nesse sentido, preocupante a decisão do Superior Tribunal de Justiça, que em recente decisão da Segunda Turma, no julgamento do Aresp 2.130.619[29] assim decidiu:

> O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações.

Nos termos da LGPD, conforme o §3º do artigo 48[30], ao analisar a gravidade deverá haver a comprovação de que foram adotadas as medidas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. Ou seja, manterá longe do alcance de terceiros e utilizará métodos já existentes de prevenção como senhas, criptografia, dentre outros, para inibir eventual vazamento.

---

[29] BRASIL. Superior Tribunal de Justiça. AResp 2.130.619. Segunda Turma. Disponível em: <https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788®istro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF> Acesso 11 ago. 2023.

[30] BRASIL. Lei 13709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados no Brasil. Disponível em: <<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 ago. 2023.

Ainda, conforme o artigo 46[31] da LGPD há o dever de que medidas de segurança sejam implementadas pelos agentes de tratamento de dados, inibindo acessos não autorizados e dificultando a interpretação dos dados em caso de perda ou acesso indevido. Há desta forma o dever de realizar medidas preventivas de segurança, sejam softwares, *hardwares* e ainda, ação humana, através de treinamentos para os agentes que trabalham com tais dados.

Portanto, é de suma importância a adoção de um sistema de *compliance* que abranja as boas práticas corporativas e as regulamentações trazidas com o advento da Lei Geral de Proteção de Dados, tanto em um aspecto de prevenção quanto de punição, em caso de não funcionamento adequado do primeiro.

CONCLUSÃO

Verifica-se, dessa maneira, que o conceito atual de privacidade está ligado à autodeterminação informativa trazendo o controle das informações, apesar de compartilhadas, para o seu titular.

A breve análise de alguns riscos envolvendo a privacidade na sociedade da informação e observação de como, sem a devida regulamentação, o usuário torna-se refém de quem detém as suas informações, dificultando até mesmo comprovar infração ao seu direito, como uso indevido, compartilhamento, ausência de consentimento para o tratamento dos dados, pouco investimento em segurança e capacitação para gerenciar os dados de terceiros.

A tecnologia está se desenvolvendo a todo o momento e a legislação que regulamenta o seu uso deve acompanhá-la, não podendo haver novo espaço virtual sem a devida regulação. Todavia, a LGPD chegou tarde para proteger os usuários da internet.

O que se espera é que venha a inaugurar um novo momento de conscientização, tanto por parte dos legisladores, do poder judiciário, dos agentes

---

[31] BRASIL. Lei 13709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados no Brasil. Disponível em: <<https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 ago. 2023.

de tratamento de dados e dos próprios usuários, que devem exigir que seja colocada em prática a devida proteção a seus direitos.

Isto porque, com a fiscalização e a colocação em prática das sanções previstas na LGPD haverá maior respeito por parte das organizações ao tratar dados de terceiros, assim como dos próprios usuários de auxiliar a fiscalizar o que está sendo feito com seus dados e denunciar quando houver violações.

REFERÊNCIAS

BARBOSA, Danilo Ricardo Ferreira; SILVA, Carlos Sérgio Gurgel. A Coleta e o uso indevido de dados pessoais: um panorama sobre a tutela da privacidade no Brasil e a Lei Geral De Proteção De Dados. Ano 5 (2019), nº 6, 473-514. Disponível em <https://www.cidp.pt/revistas/rjlb/2019/6/2019_06_0473_0514.pdf> Acesso 10 ago. 2023.

BIONI, Bruno Ricardo. E LUCIANO, Maria. O Consentimento como Processo: Em busca do consentimento válido in Tratado de Proteção de Dados Pessoais. Coord. Laura Schertel Mendes. Danilo Doneda. Ingo Wolfgang Sarlet. Otavio Luiz Rodrigues Jr.

BONNA, Alexandre Pereira; CÃNIZO, Amanda de Moura; CALZAVARA, Giovana Ferreira. Consentimento LGPD: Desafios diante da hipervulnerabilidade do Consumidor. Disponível em: <https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231/2527> Acesso 10 ago. 2023.

_____BRASIL. Lei 13709, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 10 ago. 2023.

____BRASIL. Constituição Federal de 1988. Disponível em <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso 11 de ago. 2023.

BRASIL. Superior Tribunal de Justiça. AResp 2.130.619. Segunda Turma. Disponível em <https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=178204788®istro_numero=202201522622&peticao_numero=&publicacao_data=20230310&formato=PDF> Acesso 11 ago. 2023.

CASTELLS, Manuel. A Sociedade em Rede. Volume I. 8 edição. Disponível em <https://perguntasaopo.files.wordpress.com/2011/02/castells_1999_parte1_cap1.pdf> Acesso em 07 de agosto de 2023.

DONEDA, Danilo. Da Privacidade à Proteção de Dados Pessoais. Disponível em <https://www.portaldeperiodicos.idp.edu.br/rda/article/view/6231/2527> Acesso 09 ago. 2023.

LIMA, Francisco Rodolfo Vilela. Internet: do início a era semântica Disponível em <https://biblioteca.univap.br/dados/00003d/00003da9.pdf>. Acesso em 07 agosto de 2023.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Editora Saraiva, 2014.

OLIVEIRA, J. V; SILVA, L. A. "É de Comer?" Cookies de Navegador e os Desafios à Privacidade na Rede. R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, jul./set. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/download/8419/6309>. Acesso em: 07 ago. 2023.

O'NEIL, CATHY. Algorítimos de Destruição em Massa. 2020.

PAIVA, Olívia Caetano Salgado. O Direito à Intimidade nas Relações Conjugais Versus Contratualização do Casamento. Direito de família e sucessões I [Recurso eletrônico on-line] organização CONPEDI/UNICURITIBA; Coordenadores: Sergio Pereira Braga, Tereza Cristina Monteiro Mafra, Valéria Silva Galdino Cardin – Florianópolis: CONPEDI, 2016.

PEZZI, Ana Paula Jacobus. A necessidade de proteção dos dados pessoais nos arquivos de consumo: em busca da concretização do direito à privacidade. Disponível em:
<http://www.dominiopublico.gov.br/download/teste/arqs/cp042824.pdf> Acesso 10 ago. 2023.

PILAR DA SILVA, Denise Ranghetti; STEIN, Lilian Milnitsky. Segurança da informação: uma reflexão sobre o componente humano. Ciênc. cogn., Rio de Janeiro , v. 10, p. 46-53, mar. 2007. Disponível em: <http://pepsic.bvsalud.org/scielo.php?script=sci_arttext&pid=S1806-58212007000100006&lng=pt&nrm=iso> acessos em 07 ago. 2023.

RODOTÀ, Stefano. A vida na sociedade da vigilância – a privacidade hoje. Maria Celina Bodin de Moraes (org.). Rio de Janeiro: Renovar, 2008.

ZUBOFF, Shoshana. A Era do Capitalismo de Vigilância. Intrínseca, 2021.

WERTHEIN, Jorge. A Sociedade da Informação e seus desafios. Disponível em <https://www.scielo.br/j/ci/a/rmmLFLLbYsjPrkNrbkrK7VF/?format=pdf&lang=pt> Acesso em: 07 agosto 2023.

7. DADOS PESSOAIS SENSÍVEIS: PROBLEMÁTICAS APLICADAS

https://doi.org/10.36592/9786554600712-07

Pedro Guilherme Müller Kurban[1]

SUMÁRIO

1. Introdução; 2. Dados sensíveis: definições e conceitos; 3. Direito Fundamental: banco de dados para formação de perfis e discriminação; 4. Direito do consumidor e credit scoring; 5. Dados de saúde e genéticos; 5.1 Operadoras de planos; 5.2 Pesquisas genéticas e vigilância; 5.3 COVID-19 e passaporte vacinal; 6. Dado sobre opinião política: sistema DivulgaCandContas; 7. Biometria eleitoral para fins investigatórios; 8. Conclusão.

RESUMO

O presente trabalho procura traçar um panorama geral acerca do tratamento dispensado pela Lei Geral de Proteção de Dados (LGPD) quanto aos dados pessoais sensíveis. Para tanto, adotou-se o método de abordagem indutivo, conceituando-os e delimitando-os, bem como trazendo à baila posições pertinentes à temática e problemáticas dela decorrentes pelos procedimentos tipológico e funcionalista, a fim de contextualizar o estado da arte da matéria, interpretando-o de forma exegética e sociológica a partir de questões aplicadas.
Palavras-chave: Dados Pessoais Sensíveis; LGPD; Taxatividade; Saúde; Eleitoral; Biometria.

1 INTRODUÇÃO

A temática dos dados pessoais sensíveis demanda investigação e aprofundamento teórico, considerando que há uma gama extensa de possibilidades a serem exploradas e examinadas, intensificando-se na sociedade tecnológica, cuja dinâmica de transmissão de dados é ininterrupta em um fluxo frenético, no qual os dados pessoais sensíveis ganham relevo por sua natureza ímpar.

[1] Advogado. Mestrando em Direito pela Escola de Direito da PUCRS. Especialista em Ciências Penais pela PUCRS. Especializando em Direito Eleitoral pela PUCMG.
Email: pedro@deliapiresadvogados.com.br.

Nessa toada, verifica-se que um dos elementos preponderantes e recorrentemente referidos na doutrina é o caráter de perpetuidade e de perenidade dos dados pessoais sensíveis; muito mais do que se trabalhar o rol fixado pelo legislador na LGPD, o conceito dos dados sensíveis se entrelaça com os riscos do seu mau uso, acarretando o perigo da irreversibilidade em desvios da finalidade precípua de sua coleta, e o consequente prejuízo *ad aeternum* que pode representar aos seus titulares, uma vez que intrinsicamente vinculados à sua personalidade e à própria essência do seu ser.

Tendo esse norte, buscar-se-á discorrer e problematizar, através do procedimento tipológico, algumas questões atuais atinentes aos dados pessoais sensíveis, e, por meio do método indutivo, conceitos e definições, mas também propondo-se, pelo procedimento finalista, inseri-los no contexto de aplicação em uma realidade que já se apresenta, tanto no mundo jurídico, quanto no cotidiano, posto ser um fenômeno social amplo. Entretanto, considerando a extensão e a multiplicidade do tema, este trabalho não tem a pretensão de exaurir a matéria ou fornecer respostas peremptórias até porque o assunto permanece em constante movimento, altamente passível de alterações e de adaptações em conformidade com as disrupções diariamente ocorridas no âmago da sociedade.

Enfim, o estudo dos dados pessoais sensíveis é imprescindível e, ao mesmo tempo, desafiador. Por esse motivo, delinear-se-á o quadro geral a partir de trabalhos existentes, respigar-se-ão elementos jurisprudenciais para que se possa projetar, ao menos em nível de prognóstico, o seu tratamento perante os tribunais, malgrado ainda serem incipientes, assim como coligir-se-ão tópicos controversos que envolvam o objeto a fim de ampliar a sua perspectiva de discussão.

2 DADOS SENSÍVEIS: DEFINIÇÕES E CONCEITOS

Primeiramente, destaca-se que o inciso II do artigo 5º, da Lei n.º 13.709/18 (LGPD) é bastante claro quanto ao conceito de dado pessoal sensível, como aliás o é em relação às demais definições abarcadas por essa legislação; segundo a expressa dicção legal, dado pessoal sensível é aquele “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a

organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"[2]. Insere-se dentro do escopo da LGPD, que "tem como objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[3].

Ademais, é cediço que a proteção dos dados pessoais é um direito fundamental, mais ainda, a fundamentalidade desse direito se interrelaciona intrinsicamente com a proteção da dignidade da pessoa humana:

> No que toca aos dados sensíveis, reafirma-se a exigência de uma proteção especial alicerçada no princípio da dignidade da pessoa humana, cuja fundamentalidade ainda radica e sustenta a própria ideia contemporânea de democracia e o atual molde de Estado de Direito.[4]

Os dados pessoais sensíveis são merecedores de tratamento mais pormenorizado e distinto por seu caráter especial, e "o adjetivo 'sensíveis' advém da proteção especial que carece o manejo de tal espécie de informação. Contudo, mais importante do que as informações que revelam é o fim a que atendem"[5], registrando que "eventual incidente de segurança com esses tipos de dados pode trazer consequências mais gravosas aos direitos e liberdades dos titulares"[6], calhando mencionar o potencial claro de mau uso desses dados para fins discriminatórios:

---

[2] BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

[3] FLEMING, Maria Cristina. LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis. **Conjur**, São Paulo, SP, 6 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis. Acesso em: 10 abr. 2023.

[4] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 196. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

[5] LONGHI, João Victor Rozatti. **Responsabilidade civil e redes sociais**: retirada de conteúdo, perfis falsos, discurso de ódio e fake news. Indaiatuba, SP: Editora Foco, 2020. p. 97.

[6] FLEMING, Maria Cristina. LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis. **Conjur**, São Paulo, SP, 6 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis. Acesso em: 10 abr.2023.

> Fala-se em dados pessoais sensíveis aqueles que poderiam de alguma forma gerar discriminação, como, por exemplo: origem racial, opiniões políticas, opção religiosa, dados de saúde, opção sexual, biometria, dentre outros. Dados como a íris, a voz ou a digital de uma pessoa também são considerados dados sensíveis, na medida em que, se vazados, poderão causar danos ao titular pelo resto da vida, ante a impossibilidade de se dissociar esses dados do seu titular.[7]

Por outra vertente, importa pontuar-se que:

> A proteção dos dados pessoais deve resguardar igualmente todos os dados – sensíveis ou não – que possam vir a fornecer informações pessoais sobre o indivíduo. Isto porque, no atual estágio de desenvolvimento tecnológico, dados aparentemente irrelevantes poderão, ao ser combinados com outros dados, resultar em informações sensíveis. Tal entendimento, contudo, não impede a constatação de que a proteção dos dados pessoais deverá ser diferenciada a depender da finalidade e da forma como será o seu tratamento – e não apenas de sua natureza sensível ou não no momento da coleta –, repercutindo, portanto, sobre as possíveis restrições a esse direito.[8]

Ainda quanto à discriminação, a proibição da utilização dos dados pessoais sensíveis para essa finalidade também é realçada por Ruaro e Sarlet:

> Outro aspecto notável foi o fortalecimento da proteção e a decorrente vedação de uso de dados sensíveis para fins discriminatórios independentemente do consentimento do usuário, especialmente em face dos riscos de destruição, de divulgação e de acesso indevido em razão da estrutura aberta da internet.[9]

---

[7] TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Comentada Artigo por Artigo. São Paulo: Editora Saraiva, 2022. p. 26. *E-book*. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 30 mar. 2023.

[8] RODRIGUES, Ricardo Schneider; RUARO, Regina Linden. O serviço remunerado de conferência de dados por biometria à luz do direito fundamental à proteção de dados pessoais: a aplicação da lei nº 13.444/2017 pelo TSE. **Revista Jurídica Luso-Brasileira (RJLB)**, Lisboa, n.3, ano 7, p.1291-1331, 2021. p. 1316.

[9] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção**

Considerando a natureza desses dados envolvidos, a legislação outorgou tratamento diferenciado e tutela específica para o rol daqueles classificados como sensíveis:

> Os dados pessoais sensíveis, como já definidos anteriormente, demandam uma tutela maior, o que significa que, para seu tratamento, exigir-se-á um maior rigor. O artigo em comento especifica em rol taxativo quais as hipóteses possíveis para seu tratamento, que serão, ou quando o titular consentir especificamente e de forma destacada (I), ou para as hipóteses específicas do inciso II, em que a sua utilização, mesmo sem o consentimento, se justifica pelo bem do próprio titular ou da coletividade, desde que a utilização dos dados pessoais sensíveis seja indispensável para isso.[10]

O Superior Tribunal de Justiça indicou que o catálogo dos dados pessoais sensíveis do Artigo 5º da LGPD é taxativo.[11] Ora, "o conceito de dado pessoal sensível em razão de sua especialidade e das diversas restrições impostas ao seu tratamento é taxativo."[12] Para fins de dano moral, referido Tribunal recentemente julgou caso sobre a matéria assentando *in verbis*:

> O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da

de Dados Pessoais. Rio de Janeiro: Forense, 2021. p. 206. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

[10] TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. São Paulo: Editora Saraiva, 2022, p. 26. *E-book*. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 30 mar. 2023.

[11] BRASIL. Superior Tribunal de Justiça (Segunda Turma). **Agravo em Recurso Especial n. 2.130.619/SP**. PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. Relator: Min. Francisco Falcão, 7 de março de 2023. Publicado no DJE em 10 mar.2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 05 abr. 2023.

[12] FLEMING, Maria Cristina. LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis. **Conjur**, São Paulo, SP, 6 mar. 2021. Disponível em: https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis. Acesso em: 10 abr. 2023.

> exposição dessas informações. **Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural** [grifo nosso][13].

Mesmo que incipientemente, pode-se perceber que o STJ tenciona circunscrever as hipóteses geradoras de dano moral em decorrência de vazamento de dados. Giza-se que os casos de vazamento de dados pessoais têm-se tornado mais comuns, o que se explica pelo crescente uso e transmissão de dados na sociedade tecnológica, onde a sua consectária judicialização acabará acompanhando esse crescimento.

Nesse diapasão, aventa-se que os tribunais tenderão a fixar parâmetros para a responsabilização dos agentes de tratamento dos dados pessoais com o fito de evitar um alastramento de ações nesse jaez intentando reparações de ordem pecuniária. O acórdão do Superior Tribunal de Justiça referido alhures demonstra que não é qualquer vazamento passível de gerar dano moral, mas avaliza uma construção pretoriana inicial no sentido de dano *in re ipsa* atrelado aos dados pessoais sensíveis. Como mencionado, qualquer conclusão pode ser prematura, ainda mais que a decisão analisada pode tão somente ter-se fundamentado desse modo visando repelir a incidência da indenização, valendo-se das circunstâncias do caso concreto em que os dados pessoais sensíveis não estavam envolvidos.

Todavia, cabe uma reflexão sobre a forma mais adequada de aquilatar a responsabilização pelo mau uso dos dados pessoais sensíveis que não pela perspectiva restritivamente financista, buscando averiguar os critérios não só do dimensionamento do dano, mas também da sua consequência. Oportuno, neste talvegue, a obra de Anderson Schreiber [14] acerca dos novos paradigmas da responsabilidade civil, ao que vale estender aos danos decorrentes de vazamento de dados pessoais. Com efeito, surge então o questionamento sobre como arbitrar uma

---

[13] PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. Relator: Min. Francisco Falcão, 7 de março de 2023. Publicado no DJE em 10 mar.2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023. Acesso em: 05 abr. 2023.

[14] SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 5. ed. São Paulo: Atlas, 2013.

indenização por vazamento pela ótica da dor ou do sofrimento, corriqueiramente incluídos como intrínsecos ao dano moral. Sob essa ótica refere-se que:

> A afirmação do caráter *in re ipsa* vem quase sempre vinculada a uma definição consequencialística de dano moral, muito frequentemente invocada a partir da sua associação com a dor ou o sofrimento. Sob esta ótica, parece mesmo óbvio que a prova do dano deve ser dispensada [...] A verdade, no entanto, é que a dor não define, nem configura elemento hábil à definição ontológica do dano moral. Como já demonstrado, trata-se de uma mera consequência, eventual, da lesão à personalidade e que, por isso mesmo, mostra-se irrelevante à sua configuração. [15]

Assim sendo, é possível vislumbrar o dano causado por vazamento de dados pessoais, mais especificamente dados pessoais sensíveis, pelo viés da lesão à personalidade.

3 DIREITO FUNDAMENTAL: BANCO DE DADOS PARA FORMAÇÃO DE PERFIS E DISCRIMINAÇÃO

A proteção de dados é um direito fundamental, positivado no inciso LXXXI do Artigo 5º da CF, incluído pela Emenda Constitucional nº 115 de 2022[16], em razão do mencionado conteúdo atrelado à dignidade da pessoa humana:

> Pautando-se nos princípios da precaução e da prevenção, reconheceu a vinculação dos dados à pessoa humana e, de modo particular, destacou a relevância do consentimento livre, específico, atrelado a uma finalidade e fruto de um processo gnosiológico de emancipação e de informação nas operações envolvendo tráfego de dados pessoais, **sobretudo quando se trata de dados sensíveis** [grifo nosso].[17]

---

[15]*Ibid.,* p. 204-205.

[16]*In verbis:* "LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

[17]RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de

O livre desenvolvimento da personalidade, corolário da dignidade da pessoa humana, é o supedâneo da proteção ao tratamento dos dados pessoais, proteção essa potencializada diante dos dados pessoais sensíveis.

> Mas, possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana, que, de acordo com tradição jurídica já consolidada no direito constitucional estrangeiro e no direito internacional (universal e regional) dos direitos humanos, inclui o (mas não se limita ao!) direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa.[18]

Veja-se que o consentimento para o tratamento dos dados pessoais sensíveis deve contemplar destaque e especificação, e "vale pontuar que o consentimento do titular para tratamento de seus dados pessoais sensíveis, além de ser livre, inequívoco e informado, também deverá ser específico e de forma destacada, diferindo-se do consentimento de dados pessoais que não são sensíveis"[19], afora que o requerimento deste consentimento deve ser transparente e inequívoco, consoante a disposição do inciso I do Artigo 11 da LGPD[20]. Ademais, consigna-se que "o consentimento, não custa reforçar, se aplica sempre em razão de uma finalidade explicitada e específica, impossibilitando-se o uso de uma aprovação

Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 208. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

[18]SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, MG, ano 14, n. 42, p. 179-218, jan./jun. 2020. p. 185.

[19]TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo**. São Paulo: Editora Saraiva, 2022. p. 27. *E-book*. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 30 mar. 2023.

[20]*In verbis*: "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas".

genérica."[21]

Esta proteção desdobra-se numa acepção de liberdade, ou seja, liberdade do titular de ser acautelada contra intromissões de agentes controladores, tendo em vista a sociedade digitalizada. Isto porque controlar os dados pessoais, notadamente os dados pessoais sensíveis, é deveras controlar a própria pessoa:

> Mas o reforço institucional da liberdade nesta sua nova dimensão não pode valer apenas contra a intromissão dos Estados. Deve projetar-se também sobre os novos "Senhores da Informação" que, por meio das gigantescas coletas de dados, governam as nossas vidas. Em face de tudo isso, a palavra "*privacy*" evoca não apenas uma necessidade de intimidade, mas sintetiza as liberdades que nos pertencem no mundo novo onde vivemos.[22]

Da proteção da liberdade decorre a autodeterminação do indivíduo, como sujeito de direitos sobre seus próprios dados e não homem-objeto; a bem dizer, sujeito sobre sua própria personalidade, sobre seu rosto e "espero que não seja exagero estender essa fenomenologia do rosto um pouco mais e ver o rosto como símbolo do indivíduo e como mostra de sua individualidade."[23] Ademais:

> Ressalte-se, por oportuno, que com isso não estamos a sustentar a equiparação entre as noções de dignidade e liberdade, já que, como veremos, a liberdade e, por consequência, o reconhecimento e a garantia de direitos de liberdade constituem uma das principais (se não a principal) exigências do princípio da dignidade da pessoa humana.[24]

---

[21]RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 205. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

[22]RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet? Tradução Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**. Rio de Janeiro, a. 4, n. 2, p. 1-8, jul.-dez./2015, p. 1. Disponível em: <http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/>. Acesso em: 10 abr. 2023. p. 1.

[23]SCRUTON, Roger. **O rosto de Deus**. Tradução Pedro Sette-Câmara. São Paulo: É Realizações, 2015. p. 124.

[24] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018. p. 103.

A objetificação em bancos de dados nada mais é do que a supressão do rosto, e:

> A proteção dos dados pessoais sensíveis está, dentro desse quadro, diretamente relacionada à autodeterminação informativa, em especial quando se tem em mente que o controle e o compartilhamento destes se tornou essencial nos dias de hoje para o livre desenvolvimento da personalidade em uma sociedade assentada na economia de dados e em um contexto marcadamente voltado para a vigilância e para o tecnocontrole.[25]

Sendo um direito fundamental, o tratamento de dados pessoais sensíveis merece ser resguardado de compilação indevida para a constituição de banco de dados, cuja serventia desborde do expresso interesse do titular dos dados, que se materializa através do consentimento. Nesse sentido, "a coleta e armazenamento de dados sensíveis na sociedade de consumo não pode ser concebida sob a perspectiva abstrata e sim em concreto".[26] Eventual desvio pode representar vantagem econômica para quem detenha os dados do titular em detrimento deste, e:

> Bancos de dados são, em sua acepção fundamental, um conjunto de informações estruturado de acordo com uma determinada lógica – e esta lógica é sempre uma lógica utilitarista, uma lógica que procura proporcionar a extração do máximo de proveito possível a partir de um conjunto de informações.[27]

A reunião de dados pessoais sensíveis visando à formação de perfis é social e democraticamente danosa, demandando salvaguarda ímpar em um pretendido Estado Democrático de Direito:

---

[25]RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 208. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.
[26]LONGHI, João Victor Rozatti. **Responsabilidade civil e redes sociais**: retirada de conteúdo, perfis falsos, discurso de ódio e fake news. Indaiatuba, SP: Editora Foco, 2020. p. 97.
[27]DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011. p. 92.

> Dados referentes aos hábitos alimentares, à saúde, à identidade genética, entre outros, podem vir a ser utilizados para a composição de perfis para fins discriminatórios, portanto, utilizados para fins de caráter inaceitável e injustificável em regimes democráticos e, dessa forma, a noção acerca dos dados sensíveis pode vir a ser radicalmente alterada, carecendo de maior proteção, que deve se manter sempre atualizada e em constante atualização.[28]

Mister, pois, ter-se cuidado redobrado no tratamento dos dados pessoais sensíveis visando obstar a construção destes bancos de dados.

4 DIREITO DO CONSUMIDOR E CREDIT SCORING

Ainda no âmbito da formação de bancos de dados a partir dos dados pessoais, valioso recordar a lição do então Ministro do STJ, Ruy Rosado de Aguiar, que, em decisão judicial datada de mais de vinte anos antes da promulgação da LGPD, anteviu o risco representado pelos bancos de dados como ameaça à vida privada por desvelar a conduta do cidadão em verdadeira devassa. O fundamento decisório do ministro constituiu supedâneo vanguardista da ulterior proteção no tratamento de dados dispensada pelo ordenamento jurídico pátrio, como se infere:

> A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais [...] E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins

---

[28] RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. p. 208. *E-book*. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

> contrários à moral ou ao Direito, **como instrumento de perseguição política ou opressão econômica** [grifo nosso].[29]

Consigna-se o aparato do direito consumerista acerca da prática de bancos de dados de crédito, notadamente a Seção VI o Código de Direito do Consumidor, sendo possível considerar verdadeiro marco normativo a sedimentar a futura legislação de proteção de dados. Observe-se que:

> Na legislação infraconstitucional, destaque-se o Código de Defesa do Consumidor, Lei 8.078/90, cujo artigo 43 estabelece uma série de direitos e garantias para o consumidor em relação às suas informações pessoais presentes em "bancos de dados e cadastros", implementando uma sistemática baseada nos *Fair Information Principles* à matéria de concessão de crédito e possibilitando que parte da doutrina verifique neste texto legal o marco normativo dos princípios de proteção de dados pessoais no direito brasileiro.[30]

De uma primeira leitura, constata-se que o inciso II do Artigo 5º da LGPD, malgrado abrangente, não outorga o caráter de dado sensível às informações concernentes à consulta de proteção ao crédito, as quais, a despeito de terem o condão de acarretar exposição íntima da pessoa natural, estão excluídos do âmbito de proteção da norma para tratamento especial e diferenciado.

Neste talvegue, importa arrolar recente julgado do Tribunal de Justiça do Estado do Rio Grande do Sul, segundo o qual os dados pessoais financeiros "não gozam de sigilo, eis que possuem a finalidade de proteção ao crédito", ressaltando, acerca do acesso aos bancos de dados de crédito como o SCPC e o SERASA, que "a consulta é confidencial e direcionada àqueles atores que ofertam crédito no

---

[29] BRASIL. Superior Tribunal de Justiça (Quarta Turma). **Recurso Especial n. 22.337/RS**. SERVIÇO DE PROTEÇÃO AO CRÉDITO. CANCELAMENTO DO REGISTRO. PRAZO (CINCO ANOS). O REGISTRO DE DADOS NO SPC DEVE SER CANCELADO APÓS CINCO ANOS. ART. 43, PARAGRAFO 1, DO CODIGO DE DEFESA DO CONSUMIDOR (LEI 8.078/90). Relator: Min. Ruy Rosado de Aguiar, 13 de fevereiro de 1995, Brasília, DF. Publicado no Diário da Justiça em:
20mar.1995. p. 6119. Disponível em: https://processo.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=&formato=PDF. Acesso em: 25 abr. 2023.

[30] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011. p. 103.

mercado"[31]. Dada a incipiência da LGPD, os julgados ainda são raros; entretanto, cumpre compilar os entendimentos que já vêm-se formando para compreender a dinâmica que a jurisprudência outorgará à matéria. Este entendimento do Tribunal de Justiça do Rio Grande do Sul espelha-se em parte no Superior Tribunal de Justiça que, em acórdão paradigmático, avalizou o sistema de "*credit scoring*", considerando-o "um método desenvolvido para avaliação do risco de concessão de crédito"[32], confirmando a licitude desta prática comercial com base na Lei 12.414/2011, a chamada lei do cadastro positivo, pontuando ser "desnecessário o consentimento do consumidor consultado", ainda que se lhe deva outorgar "esclarecimentos, caso solicitados, acerca das fontes dos dados considerados (histórico de crédito), bem como as informações pessoais valorada."

5 DADOS DE SAÚDE E GENÉTICOS

Por seu turno, interessa perscrutar as perspectivas dos dados pessoais sensíveis de saúde e genéticos, assim como as problemáticas deles advindas, investigando-se seus riscos para equilibrar-se com os benefícios de eventuais avanços tecnológicos e medicinais.

5.1 OPERADORAS DE PLANOS

Os dados referentes à saúde também são considerados sensíveis, e recebem maior atenção pela tensão inerente com as operadoras de planos de saúde e sua

[31] RIO GRANDE DO SUL. Tribunal de Justiça (Décima Câmara Cível). **Apelação Cível nº 51393545820218210001**. APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA CUMULADA COM OBRIGAÇÃO DE FAZER E INDENIZAÇÃO POR DANOS MORAIS. VEICULAÇÃO DE INFORMAÇÕES EM CONSULTA DE CRÉDITO. AUSÊNCIA DE ILEGALIDADE DO REGISTRO.LGPD. Relator: Des. Jorge Alberto Schreiner Pestana, 23 fev.2023. Publicado no DJE em 2 7 fev.2023. Disponível em: https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php. Acesso e m: 17 mar. 2023.

[32]BRASIL, Superior Tribunal de Justiça (Segunda Seção). **Recurso Especial (Resp) n.1.419.697/RS**. RECURSO ESPECIAL REPRESENTATIVO DE CONTROVÉRSIA (ART. 543-C DO CPC). TEMA 710/STJ. DIREITO DO CONSUMIDOR. ARQUIVOS DE CRÉDITO. SISTEMA "CREDIT SCORING". COMPATIBILIDADE COM O DIREITO BRASILEIRO. LIMITES. DANO MORAL. Relator: Min. Paulo de Tarso Sanseverino, Brasília, DF, 12 de novembro de 2014. Publicado no DJe em 17 nov. 2014. RSTJ vol. 236. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_r egistro=201303862850&dt_publicacao=17/11/2014. Acesso em: 03 abr. 2023.

metodologia de seleção atuarial, considerando que são:

> Dados capazes de fornecer um detalhamento sobre as condições do sujeito, o que poderia levar planos privados a selecionarem segurados conforme os riscos que oferecem. A LGPD, nesse sentido, é categórica ao vedar o tratamento desses dados para fins de seleção de risco nas contratações das diversas modalidades dos planos de saúde. Ademais, a proibição de tal prática inviabiliza que as operadoras excluam beneficiários com base em dados pessoais sensíveis.[33]

Logo, esses dados de saúde demandam explícita finalidade tanto para coleta quanto para compartilhamento:

> Quanto aos limites e restrições, toda e qualquer captação (levantamento), armazenamento, utilização e transmissão de dados pessoais, em princípio, constitui uma intervenção no âmbito de proteção do direito, que, portanto, como já adiantado, não prescinde de adequada justificação. Outrossim, embora não se trate de direito absoluto, revela-se como um direito bastante sensível, tanto mais sensível quanto mais se tratar de dados pessoais sensíveis, associados a dimensões da dignidade da pessoa humana, implicando, de tal sorte, exigências mais rigorosas – e controle mais intenso– de eventuais intervenções restritivas.[34]

Consigna-se a vedação legal explícita do Artigo 11, § 5º, LGPD[35] para o tratamento destes dados pessoais sensíveis na formulação de planos com base na seleção de risco. Atente-se a um difícil equilíbrio entre a lógica mercadológica para estabelecimento de preço adequado e justo entre os contratantes de planos de saúde e o mau uso dos dados sensíveis para discriminação e seleção de riscos.

---

[33] BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos.** Rio de Janeiro: Lumen Juris, 2021. p. 85.

[34] SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, MG, ano 14, n. 42, p. 179-218, jan./jun. 2020. p. 210-211.

[35] Art.11 [...] § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (Incluído pela Lei nº 13.853, de 2019).

5.2 PESQUISAS GENÉTICAS E VIGILÂNCIA

Inicialmente, assevera-se a especial atenção aos dados genéticos, já que perfazem o rol de dados sensíveis, como previsto no inciso II do artigo 5º da LGPD[36]. Ora, a genética acompanha o indivíduo e lhe é indissociável; dessa forma, estes dados pessoais, uma vez extraídos, demandam acompanhamento protetivo redobrado e contínuo, pois levanta fundados receios de malversação. Assinala-se que as técnicas modernas de obtenção destes dados têm preocupado, valendo referir a possibilidade noticiada de detecção do DNA inclusive por partículas do ar[37], expondo ainda mais os indivíduos, criando um ambiente de vigilância permanente em que a própria ideia de consentimento pode ficar seriamente comprometida.

No Artigo 9º do Regulamento Geral de Proteção de Dados da União Europeia, por exemplo, a coleta de dados genéticos ou relativo à saúde é vedada, exceto para medicina preventiva ou ocupacional, bem como para o diagnóstico médico, para a prestação de cuidados ou tratamentos de saúde ou de ação social ou a gestão de sistemas e serviços de saúde, conforme a alínea "*h*" do mesmo dispositivo[38].
Quando anonimizados, os dados deixam de ser sensíveis ou pessoais, conforme o Artigo 12 da LGPD[39]; contudo, "mesmo protegendo a identificação individual, há o risco de prejuízo a grupos de pessoas, uma vez que o conjunto dos dados poderia fornecer informações sobre questões étnicas, de saúde e socioeconômicas"[40],

---

[36] BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.
[37] BROWN, Elizabeth Anne. DNA já pode ser retirado do ar. E isso preocupa. Tradução Renato Prelorentzou. **O Estado de S.Paulo e The New York Times**, Nova Iorque, EUA, ano 144, nº 47346, 4 jun. 2022. Caderno A Fundo. p. 6-7.
[38]UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD).** Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 11 abr. 2023.
[39] BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.
[40] BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos.** Rio de Janeiro: Lumen Juris, 2021. p. 84.

inclusive para o risco de reversão da anonimização. Neste ponto, a transparência e o controle do fluxo de dados genéticos são imprescindíveis para fins de se evitar os supracitados efeitos nocivos de discriminação, ou de uso comercial indevido e:

> A bioética e o biodireito surgem como mecanismos para nortear as condutas na área da pesquisa genética [...] os direitos fundamentais devem ser utilizados como limites à pesquisa genética, sempre observando o princípio da dignidade da pessoa humana. Uma das problemáticas atinentes às pesquisas genéticas é justamente o tratamento conferido a esses dados genéticos.[41]

Portanto, os controladores de dados pessoais genéticos devem implementar mecanismos de segurança para minimizar ao máximo os vazamentos, empenhando-se, quando possível, na anonimização e em rigorosos instrumentos de fiscalização. O aparato protetivo legal obviamente não pode se tornar empecilho para o desenvolvimento de pesquisas clínicas com dados genéticos, mas, ao mesmo tempo, deve ter o escopo de resguardar direitos fundamentais.

5.3 COVID-19 E PASSAPORTE VACINAL

Outro aspecto problemático e digno de tensão com a LGPD foi a exigência de comprovante vacinal – também chamado de passaporte sanitário – enquanto estratégia de enfrentamento da Covid-19. O Artigo 11, II, "f", da LGPD[42] dispensa consentimento para o tratamento e o compartilhamento destes dados pessoais sensíveis em razão da tutela da saúde, sobrepondo assim o interesse público. Compila-se que "à luz da Lei Geral de Proteção de Dados, prevalece o dever de disponibilizar os dados por meio de aplicativo em face do bem-estar da coletividade, limitando-se os impactos relacionados à privacidade e segurança do cidadão".[43]

---

[41] *Ibid*., p. 45.

[42] BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

[43] GROBÉRIO, Sandra do Carmo. MONITORA COVID-19: dever de disponibilizar dados pessoais sobre infecção em aplicativo e o direito à privacidade à luz da LGPD. **Anais de Artigos Completos do VI CIDH**,

Logo, dentro do panorama brasileiro:

> Vale observar que a LGPD oferece dispositivos capazes de regrar o uso de dados pessoais nas estratégias de enfrentamento à Covid-19, uma vez que a referida Lei admite a coleta e tratamento de dados pessoais sensíveis para uso em pesquisa de saúde. A anonimização e pseudoanonimização (atribuição de um código ao indivíduo), nesse sentido, são formas de garantir a preservação da identidade do sujeito, desde que observadas normas de segurança. Assim, reforça-se também a necessidade de entes públicos e privados agirem com transparência, informando sobre armazenamento e descarte, pessoas que têm acesso a dados, formas de proteção e responsabilização sobre abusos e negligências.[44]

Ao comentar o certificado vacinal da União Europeia, Batista[45] realça o tratamento das informações ali constantes, considerando serem sigilosas, pois contém dados sensíveis; logo, serão armazenadas em banco de dados seguros em cada país de origem do cidadão, implicando um dever de salvaguarda e de cautela no tratamento destes dados, ganhando maior relevância em um contexto de crise sanitária, como foi a da COVID-19. Refere ainda Batista[46] que "o problema não é, então, tão singelo como aparenta ser, bastando sua implementação por simples decreto governamental, pois traz questões mais complexas que envolvem o caráter ético e moral da certificação."

Ademais, Batista[47] também se posiciona favoravelmente ao passaporte de imunidade (certificação vacinal), enaltecendo a sua necessidade de vigilância no contexto chinês notadamente; aponta, porém, as particularidades europeias e

---

Coimbra 2021 - Volume 7. *In*: César Augusto R. Nunes *et. al*. (orgs.) [et al.] – Campinas / Jundiaí: Editora Brasílica / Edições Brasil, 2022. p. 107.

[44] BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos.** Rio de Janeiro: Lumen Juris, 2021. p. 87.

[45] BATISTA, Anderson Röhe Fontão. PASSAPORTE COVID-19: risco e bioética na era da certificação digital. **Anais de Artigos Completos do VI CIDH**, Coimbra 2021 - Volume 7. *In*: César Augusto R. Nunes *et al*. (orgs.). Campinas / Jundiaí: Editora Brasílica / Edições Brasil, 2022. p. 68.

[46] *Ibid*., p. 70.

[47] BATISTA, Anderson Röhe Fontão. PASSAPORTE COVID-19: risco e bioética na era da certificação digital. **Anais de Artigos Completos do VI CIDH**, Coimbra 2021 - Volume 7. *In*: César Augusto R. Nunes *et al*. (orgs.). Campinas / Jundiaí: Editora Brasílica / Edições Brasil, 2022. p. 70.

estadunidenses, problematizando a possibilidade de se encontrarem outros meios mais razoáveis e menos invasivos para vigilância:

> A proporcionalidade se mostra como mais adequada para verificar se a obrigatoriedade de incluir no aplicativo dados sobre infecção por Covid-19 limita o direito à privacidade, pois há uma relação de causalidade direta entre o meio, que é o dever imposto ao cidadão, e o fim que se pretende com esse dever, que é a contribuição para o direito à saúde para toda a coletividade.[48]

Não se perca de perspectiva que o Poder Público, normalmente por decretos, delegou às pessoas jurídicas de direito privado o controle de entrada em seus estabelecimentos condicionando-os aos comprovantes vacinais, cujas informações – que são dados pessoais sensíveis – passaram ao controle destas empresas. Assim, o tratamento, a guarda e o eventual descarte se submetem ao regime da LGPD, bem como devem ser adotadas todas as medidas necessárias para evitar vazamentos e desvios de finalidade da coleta inicial.

6 DADO SOBRE OPINIÃO POLÍTICA: SISTEMA DivulgaCandContas

O Tribunal Superior Eleitoral (TSE) divulga publicamente a lista de doadores de campanha eleitoral em seu sítio eletrônico através da plataforma DivulgaCandContas[49], na qual vêm discriminados o nome e o CPF do doador, assim como a quantia doada e o destinatário da respectiva doação. O CPF, apesar de ser dado pessoal, não se encontra abrigado no inciso II do Artigo 5º da LGPD; portanto, não se trata de dado pessoal sensível, não gozando, pois, da proteção outorgada a este, mesmo que mereça a proteção geral conferida pela LGPD. No entanto, surge a problemática a respeito da opinião política do doador, uma vez que esta, sim,

[48] GROBÉRIO, Sandra do Carmo. MONITORA COVID-19: dever de disponibilizar dados pessoais sobre infecção em aplicativo e o direito à privacidade à luz da LGPD. **Anais de Artigos Completos do VI CIDH,** Coimbra 2021 - Volume 7. *In*: César Augusto R. Nunes *et. al*. (orgs.) [et al.] – Campinas / Jundiaí: Editora Brasílica / Edições Brasil, 2022. p. 106.

[49] Trata-se de plataforma disponibilizada pelo TSE em seu sítio eletrônico. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Agosto/divulgacandcontas-consulte-arrecadacoes-e-gastos-de-campanhas-nas-eleicoes-2022. Acesso em: 21 maio 2023.

enquadra-se no conceito legal de dado pessoal sensível. Veja-se que a ampla exposição pública dos doadores patrocinada pelo TSE levanta dúvidas sobre o tratamento deste dado pessoal sensível, restando a indagação sobre o consentimento do doador e sobre a forma em que esta informação pessoal é apresentada.

Como é de sabença, a Justiça Eleitoral possui função quádrupla: jurisdicional, normativa (regulamentar), consultiva e administrativa e "em cada uma das suas complexas competências, a Justiça Eleitoral brasileira prima pela transparência"[50]. Esclarece-se que essa divulgação de doações e de doadores por parte do TSE se insere nesta última função – a função administrativa. Assim procedendo, o TSE procura zelar pela maior transparência possível ao público, fundando-se no Artigo 21 da Resolução 23.607/19 do TSE[51], além da Lei n.º 12.527/11 (Lei de acesso à informação)[52], e visa atender a princípios caros ao Direito Eleitoral: transparência, legitimidade, vedação ao abuso do poder econômico na eleição. Os candidatos e partidos são obrigados a enviar dados relativos aos recursos financeiros recebidos para financiamento de sua campanha eleitoral em até 72 (setenta e duas) horas contadas a partir do recebimento das quantias por meio do Sistema de Prestação de Contas Eleitorais (SPCE), obrigação imposta pelo Artigo 28, § 4º, inciso I, e § 7º, da Lei 9.504/97 (Lei das Eleições)[53], e, também conforme o

---

[50] CARVALHO NETO, Tarcisio Vieira de. Transparência do processo eleitoral brasileiro. **Estudos eleitorais** (Tribunal Superior Eleitoral), Brasília, DF, vol. 1, n. 1, p. 9-27, maio/ago. 2016. p. 17-18.

[51] Art. 21. As doações de pessoas físicas e de recursos próprios somente poderão ser realizadas, inclusive pela internet, por meio de: I - **transação bancária na qual o CPF da doadora ou do doador seja obrigatoriamente identificado** [...] (grifo nosso).

[52] BRASIL. [Lei de Acesso à Informação]. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 jun. 2023.

[53] Art. 28. A prestação de contas será feita: [...] § 4o Os partidos políticos, as coligações e os candidatos são obrigados, durante as campanhas eleitorais, a divulgar em sítio criado pela Justiça Eleitoral para esse fim na rede mundial de computadores (internet): I - os recursos em dinheiro recebidos para financiamento de sua campanha eleitoral, em até 72 (setenta e duas) horas de seu recebimento. [...] § 7o As informações sobre os recursos recebidos a que se refere o § 4o **deverão ser divulgadas com a indicação dos nomes, do CPF ou CNPJ dos doadores e dos respectivos valores doados** (grifo nosso).

Artigo 47, § 3º da Resolução 23.607/19 do TSE[54], este tribunal divulgará na sua página na internet relatório financeiro a partir destes dados. "Essas informações, objetivando a transparência à sociedade, deverão ser divulgadas com a indicação do nome, do CPF [...] dos doadores e dos respectivos valores doados."[55]

Neste talvegue, a exposição auxilia na chamada a*ccountability*[56], tanto horizontal (para órgãos de fiscalização, como o MPE, demais candidatos, partidos, coligações, federações), mas também vertical – dirigida ao eleitorado, seja para controle de probidade financeira, seja para um válido controle político-ideológico. Pela *accountability* vertical, pode-se verificar se o doador ou pessoa correlata foi beneficiado pelo candidato eleito, se ocorreu eventual *quid pro quo*, além de se saber quem financia determinada pauta política, bem como se o doador é vinculado a alguma pessoa jurídica (empresa, associação, grupo de pessoas) e de qual agenda comunga, pois:

> A publicidade máxima da movimentação financeira de uma campanha eleitoral e mesmo partidária é um arquétipo fundamental para que o eleitor tenha real conhecimento sobre em quem votar, porque é induvidoso o comprometimento entre o financiado e a sua fonte de recursos.[57]

Não se pode olvidar dois casos de doações eleitorais que ganharam repercussão midiática durante a última eleição em 2022: a doação atribuída ao juiz

---

[54] Art. 47. Os partidos políticos e as candidatas ou os candidatos são obrigadas(os), durante as campanhas eleitorais, a enviar por meio do SPCE à Justiça Eleitoral, para divulgação em página criada na internet para esse fim (Lei nº 9.504/1997, art. 28, § 4º) : [...] § 3º O relatório financeiro de campanha será disponibilizado pelo Tribunal Superior Eleitoral na sua página na internet em até 48 (quarenta e oito) horas, ocasião em que poderão ser divulgados também os gastos eleitorais declarados, bem como as doações estimáveis em dinheiro, observado o disposto no art. 103 desta Resolução. (Redação dada pela Resolução nº 23.665/2021).

[55] OLIVEIRA, Bruno Ferreira de. Prestação de contas eleitorais e a não identificação de doadores do art. 28, § 12, da lei das eleições: análise da medida cautelar em ação direta de inconstitucionalidade nº 5.394/DF. **Estudos eleitorais** (Tribunal Superior Eleitoral), Brasília, DF, vol. 1, n. 1, p. 151-171, maio/ago. 2016. p. 154.

[56] O termo pode ser definido sinteticamente como verdadeira prestação de contas para fiscalização, na acepção de dar satisfação com a maior transparência possível ao eleitorado ou aos órgãos de controle, sem que este conceito se confunda com o processo de prestação de contas em si.

[57] OLIVEIRA, Bruno Ferreira de. Prestação de contas eleitorais e a não identificação de doadores do art. 28, § 12, da lei das eleições: análise da medida cautelar em ação direta de inconstitucionalidade nº 5.394/DF. **Estudos eleitorais** (Tribunal Superior Eleitoral), Brasília, DF, vol. 1, n. 1, p. 151-171, maio/ago.2016. p. 158.

Eduardo Appio, então titular da 13ª Vara Federal de Curitiba – conhecida como jurisdição da Operação Lava Jato – de R$ 13,00 (treze reais) à campanha presidencial de Lula[58], assim como a doação de R$ 1.000.000,00 (um milhão de reais) dos donos da marca de detergentes Ypê à campanha presidencial de Jair Bolsonaro[59]. Estas informações vieram à tona para o debate público graças à sistematização do TSE, revelando-se importante instrumento de cidadania e da democracia, além de claro controle sociopolítico, até mesmo para boicotar ou apoiar quem financia determinado candidato.

Todo interessado (mesmo não eleitor, mesmo de outra circunscrição) pode apresentar comunicação à Justiça Eleitoral ou ao MPE para impugnar as contas eleitorais e as doações, conforme Artigo 56 da Resolução 23.607/19 do TSE[60], além dos demais partidos, coligações e federações, proporcionando um controle sistêmico entre os próprios atores eleitorais. A exposição da lista de valores e de doadores possibilita identificar eventuais irregularidades, a saber: se os limites de gastos por doador ou teto de gastos de candidato foram ultrapassados[61]; eventual camuflagem ou fraude contábil - caixa dois, uso de laranjas, uso de fontes vedadas (recursos de origem estrangeira pessoas jurídicas, entes públicos, autoridades

---

[58] NOVO juiz da lava jato doou R$ 13 para a campanha de Lula. **Poder360**, 17 fev. 2023. Disponível em: https://www.poder360.com.br/justica/novo-juiz-da-lava-jato-doou-r-13-para-a-campanha-de-lula/. Acesso em: 21 maio 2023.

[59] INTERNAUTAS pedem boicote à YPÊ após doações de donos a Bolsonaro. **Poder360**, 17 out. 20222. Disponível em: https://www.poder360.com.br/eleicoes/internautas-pedem-boicote-a-ype-apos-doacoes-de-donos-a-bolsonaro/. Acesso em: 21 maio 2023.

[60] Art. 56. Com a apresentação das contas finais, a Justiça Eleitoral disponibilizará as informações a que se refere o inciso I do caput do art. 53 desta Resolução, bem como os extratos eletrônicos encaminhados à Justiça Eleitoral, na página do TSE na internet, e determinará a imediata publicação de edital para que qualquer partido político, candidata ou candidato ou coligação, o Ministério Público, bem como qualquer outra interessada ou outro interessado possam impugná-las no prazo de 3 (três) dias. § 1º A impugnação à prestação de contas deve ser formulada em petição fundamentada dirigida à relatora ou ao relator ou à juíza ou ao juiz eleitoral, relatando fatos e indicando provas, indícios e circunstâncias. § 2º As impugnações à prestação de contas das candidatas ou dos candidatos e dos respectivos partidos políticos, inclusive dos coligados, serão juntadas aos próprios autos da prestação de contas, e o cartório eleitoral ou a Secretaria do Tribunal notificará imediatamente a candidata ou o candidato ou o órgão partidário para manifestação no prazo de 3 (três) dias. § 3º Apresentada, ou não, a manifestação da impugnada ou do impugnado, transcorrido o prazo previsto no § 2º deste artigo, o cartório eleitoral ou a Secretaria do Tribunal cientificará o Ministério Público da impugnação, caso o órgão não seja o impugnante. § 4º A disponibilização das informações previstas no caput, bem como a apresentação, ou não, de impugnação não impedem a atuação do Ministério Público como custos legis nem o exame das contas pela unidade técnica ou pela(o) responsável por sua análise no cartório eleitoral.

[61] Cujos tetos máximos vêm dispostos nos parágrafos do Artigo 23 da Lei 9.504/97 (Lei das Eleições).

públicas, sindicatos, entidades beneficentes e religiosas, entidades esportivas, organizações não-governamentais que recebam recursos públicos) ou recursos de origem não identificada (RONI)[62], fornecendo ampla capacidade para rastreio dos recursos. Neste sentido, registra-se que as doações devem sempre ser identificadas e feitas em conta específica da campanha, na forma do Artigo 7º da Resolução 23.607/19 do TSE[63].

Por isso, esta lista deve vir discriminada na prestação de contas de partidos e candidatos, pois é processo, é jurisdicional, e é público. Ainda, o Artigo 103 da mesma Resolução n.º 23.607/19 dispõe que os processos de prestação de contas são públicos e podem ser consultados por qualquer interessado, observadas as diretrizes para tratamento de dados pessoais da LGPD[64]. José Jairo Gomes menciona ser:

> Direito impostergável dos integrantes da comunhão política saber quem financiou a campanha de seus mandatários e de que maneira esse financiamento se deu. Nessa seara, impõe-se a transparência absoluta, pois em jogo encontra-se o legítimo exercício de mandatos e consequentemente do poder estatal. Sem isso, não é possível o exercício pleno da cidadania, já que se subtrairiam do cidadão informações essenciais para a formação de sua consciência político-moral, relevantes sobretudo para que ele aprecie a estatura ético-moral de seus representantes e até mesmo para exercer o sacrossanto direito de sufrágio.[65]

Cumpre consignar que a doação eleitoral é um ato voluntário, constituindo-se

---

[62] Vide Artigo 24 da Lei 9.504/97 e Artigo 12 da Resolução 23.604/19 TSE.

[63] Art. 7º Deverá ser emitido recibo eleitoral de toda e qualquer arrecadação de recursos: [...] § 1º As doações financeiras devem ser comprovadas, obrigatoriamente, por meio de documento bancário que identifique o CPF/CNPJ das doadoras ou dos doadores, sob pena de configurar o recebimento de recursos de origem não identificada de que trata o art. 32 desta Resolução.

[64] Art. 103. Os processos de prestação de contas são públicos e podem ser consultados por qualquer interessada ou interessado, observadas as diretrizes para tratamento de dados pessoais da Lei nº 13.709 /2018 e da Resolução TSE nº 23.650/2021. (Redação dada pela Resolução nº 23.665/2021). Parágrafo único. A Justiça Eleitoral dará ampla e irrestrita publicidade ao conteúdo dos extratos eletrônicos das contas eleitorais na página do Tribunal Superior Eleitoral na internet. (Redação dada pela Resolução nº 23.665/2021).

[65] GOMES, José Jairo. **Direito Eleitoral**. 19 ed. rev. atual. Barueri, SP: Atlas, 2023. *E-book*. ISBN 9786559775330. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559775330/. Acesso em: 21 jul. 2023. p. 381.

escolha do doador, e poderia ser equiparado ao consentimento na forma do Artigo 8º, *caput*, da LGPD – “meio que demonstre a manifestação de vontade do titular"; ao se doar, o sujeito anui com a publicização dos seus dados por parte da Justiça Eleitoral, inferindo-se ser conhecedor de antemão das consequências de participação no processo eleitoral. Afinal, a doação é uma manifestação de apoiamento ao candidato.

Com efeito, o financiador de campanha eleitoral passa a ser também participante desta, submetendo-se assim aos regramentos e às exposições típicas do período eleitoral. Dessa forma, o doador não poderia invocar para si sigilo da sua contribuição financeira, pois feriria a necessidade de transparência antes descrita, e, por corolário, não haveria sigilo da sua opção política, externada com a doação. Ademais, ocultar a identidade do doador para fins de preservar a sua opção política, por analogia, equivaleria a ocultar a opção política de um candidato ou de outro ator político diretamente envolvido na campanha – quem aparecesse na propaganda eleitoral, por exemplo, o que evidentemente destoa da razoabilidade.

7 BIOMETRIA ELEITORAL PARA FINS INVESTIGATÓRIOS

Em 3 de fevereiro de 2023, o Ministro Alexandre de Moraes, nos autos do Inquérito n.º 4.923/DF do STF, autorizou a disponibilização dos dados biométricos constantes no TSE para consulta por parte da Polícia Federal a fim de identificar possíveis envolvidos nas invasões às sedes dos Três Poderes ocorridas em 8 de janeiro de 2023, e não se pode olvidar que o supracitado inciso II do Artigo 5º, LGPD define o dado biométrico como dado pessoal sensível. A coleta da biometria pela Justiça Eleitoral se relaciona ao exercício do voto, e se coaduna com os princípios eleitorais da igualdade – *one man one vote*, da legitimidade, da autenticidade e da lisura. A decisão do Ministro se lastreou na Lei 13.444/17[66] e na Resolução

[66] BRASIL. **Lei nº 13.444, de 11 de maio de 2017**. Dispõe sobre a Identificação Civil Nacional (ICN). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 24 mai. 2023.

23.656/21 do TSE[67], e apenas faz referência de que "deverão ser adotadas as medidas de segurança referidas no art. 46 da Lei 13.709/22 [sic] (Lei Geral de Proteção de Dados)"[68]. Ao comentar a Lei nº 13.444/2017, Rodrigues e Ruaro defendem que:

> Faz sentido que as polícias tenham acesso a essa informação (registro biométrico), pois imprescindível para possibilitar a correta identificação daqueles eventualmente implicados na prática de algum delito, hipótese que, inclusive, vai ao encontro do disposto no art. 5º, inciso LVIII, da Constituição.[69]

Esta intercomunicação de dados pessoais sensíveis levanta importantes questionamentos sobre a aplicação da Lei 13.709/18 (LGPD), assim como de eventual desvio de finalidade da coleta biométrica por parte do Poder Público. Não se pode olvidar que, conforme as alíneas do inciso III do Artigo 4º, a LGPD não incide em tratamento de dados voltados à segurança pública, à defesa nacional, à segurança do Estado ou a atividades de investigação e repressão de infrações penais. Portanto, em princípio, poder-se-ia falar em excludente do tratamento outorgado pela LGPD nestas hipóteses, enquadráveis na situação em comento.

De outra forma, o inciso I do Artigo 11 da LGPD estabelece que o consentimento com o tratamento de seus dados pessoais sensíveis é feito para uma finalidade determinada, o que, *a contrario sensu*, excluiria o uso e o tratamento dos dados pessoais para finalidade não consentida, considerando que "as informações que o Estado colhe coercitivamente de seus cidadãos só podem ser utilizadas para

---

[67] BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.656, de 7 de outubro de 2021**; dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados da Justiça Eleitoral (JE). Diário de Justiça Eletrônico (DJE) nº 190, Brasília, 15 de outubro de 2021, p. 90-95. Disponível em: https://sintse.tse.jus.br/documentos/2021/Out/15/diario-da-justica-eletronico-tse/resolucao-no-23-656-de-7-de-outubro-de-2021-dispoe-sobre-o-acesso-a-dados-pessoais-constantes-dos-si. Aceso em 30 mar. 2023.

[68] BRASIL. Supremo Tribunal Federal. **Inquérito nº 4923**. Relator: Min. Alexandre de Moraes, 03 de fevereiro de 2023. Publicado no DJE em 09 de fevereiro de 2023, Brasília, DF. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/INQ4929AUTORIZAaOPARACONFERIMENTODEBIOMETRIA.pdf. Acesso em: 17 abr. 2023.

[69] RODRIGUES, Ricardo Schneider; RUARO, Regina Linden. O serviço remunerado de conferência de dados por biometria à luz do direito fundamental à proteção de dados pessoais: a aplicação da lei nº 13.444/2017 pelo TSE. **Revista Jurídica Luso-Brasileira (RJLB)**, Lisboa, n.3, ano 7, p.1291-1331, 2021. p. 1323.

as específicas finalidades públicas que justificam a coleta e o armazenamento de tais dados"[70].

Veja-se que o eleitor, ao ceder a sua biometria para cadastro, consentiu na sua utilização única e exclusivamente para fins de identificação eleitoral, não para que fosse compilado em um banco de dados unificado a ser manejado consoante a oportunidade e a conveniência da Administração Pública e das suas autoridades. Por outra frente, reconhece-se que dificilmente seria fornecido consentimento para que o Poder Público usasse os dados em desfavor do titular. Assinala-se que o inciso II do mesmo Artigo 11 disciplina as hipóteses em que o tratamento dos dados pessoais se dá sem fornecimento de consentimento do titular, valendo destacar a alínea "g", cujo escopo é a "garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais":

> Para além das situações em que o indivíduo cede voluntariamente seus dados a fim de poder usufruir determinado serviço, há os casos em que essas informações não são espontaneamente fornecidas, mas exigidas por lei, armazenadas em bancos de dados, processadas e, eventualmente, difundidas para terceiros pelo poder público. Diversos problemas podem decorrer do manuseio inadequado de dados pessoais pelo poder público.[71]

Nesse sentido, virtual desvio de finalidade na utilização de dados pessoais atentaria contra os princípios expostos no Artigo 6º da LGPD, agravando-se em casos de dados pessoais de natureza sensível. Giza-se que a LGPD, em seu artigo 21, dispõe que "os dados pessoais referentes ao exercício regular de direitos pelo

---

[70] RODRIGUES, Ricardo Schneider; RUARO, Regina Linden. O serviço remunerado de conferência de dados por biometria à luz do direito fundamental à proteção de dados pessoais: a aplicação da lei nº 13.444/2017 pelo TSE. **Revista Jurídica Luso-Brasileira (RJLB)**, Lisboa, n.3, ano 7, p.1291-1331, 2021. p. 1324.

[71] *Ibid.*, p. 1295.

titular não podem ser utilizados em seu prejuízo".[72] Em consonância com os mencionados dispositivos, o Artigo 26 do mesmo diploma legal esclarece que o tratamento de dados pessoais pelo Poder Público deve também atender a finalidades específicas, determinando que sejam respeitados os princípios norteadores elencados no Artigo 6º da LGPD. Acresçam-se os parâmetros definidos pelo STF para compartilhamento e tratamento de dados entre órgãos públicos no bojo do julgamento conjunto da ADI 6.649 e da ADPF 695[73], remissivo a outro importante julgado da Corte quando da ADI 6.529.

Por derradeiro, cumpre mencionar o Projeto de Lei n.º1515/2022 (Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais), que outorga ao Ministério Público e à autoridade policial acesso aos dados cadastrais mantidos pela Justiça Eleitoral independentemente de autorização judicial.[74] O PL replica, pois, sistemática semelhante à LGPD no que toca às finalidades do tratamento para as autoridades públicas envolvidas em atividades de segurança pública e o compartilhamento de dados biométricos, por sua vez, só pode ser realizado para fins de investigação criminal ou instrução processual penal. Além disso, o projeto prevê que o tratamento de dados biométricos deve respeitar aos princípios de finalidade, adequação, necessidade, transparência, segurança e prevenção[75].

CONCLUSÃO

Pelo exposto, observa-se a variedade e a abrangência da matéria acerca dos

---

[72] BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

[73] BRASIL. Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade nº 6.649 e Arguição de Descumprimento de Preceito Fundamental nº 695**. Relator: Min. Gilmar Mendes, 15 de setembro de 2022. Publicado no DJE nº 191 em 26 de setembro de 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5938693. Acesso em: 17 abr. 2023.

[74] ARMANDO, Coronel. **Projeto de Lei da Câmara dos Deputados nº 1515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 17 abr. 2023.

[75] *Ibid.*, princípios insertos no artigo 4º do Projeto de Lei.

dados pessoais sensíveis, envolvendo diferentes vertentes do Direito, refletindo, outrossim, diversos aspectos da sociedade. De fato, a salvaguarda constitucional da proteção ao tratamento dos dados pessoais, somada à previsão de tratamento pormenorizado dos dados pessoais sensíveis pela LGPD se justifica na medida dos riscos embutidos no uso indevido destes para fins discriminatórios, além do caráter de eternidade que imprimem em casos de vazamentos.

Importa realçar o entendimento que vem se consolidando, tanto entre doutrinadores quanto na jurisprudência, de assentar ser um rol taxativo os dados pessoais sensíveis. Deveras, todo aparato legislativo e principiológico procura outorgar necessário tratamento e tutela diferenciados para os dados pessoais sensíveis.

Do mesmo modo, interessa destacar quais dados pessoais não se classificam como sensíveis e, portanto, excluem-se do seu raio específico de proteção, relevando apontar os dados de crédito – *credit scoring* – ainda que no âmbito do direito do consumidor. Na mesma toada, por outro prisma, os dados de saúde merecem proteção e tratamento específicos, especialmente em relação às operadoras de planos de saúde. O tratamento dos dados genéticos, delicados por si só, expõe a vulnerabilidade e a perpetuidade que o seu mau uso pode conduzir.

Procedeu-se à problematização do uso dos dados pessoais sensíveis em função das exigências de comprovantes de vacinação. Delimitou-se, no presente estudo, os referenciais legais para a viabilidade do uso de referidos dados, mas notadamente o eventual e necessário descarte por parte das pessoas jurídicas de direito privado a quem se outorgou o tratamento.

Instigante relatar a polêmica sobre dados relativos a opiniões políticas, tanto por se enquadrarem em dados sensíveis, por opção do legislador, quanto sua tensão em vista do sistema DivulgaCandContas disponibilizado pelo Tribunal Superior Eleitoral, que divulga com ampla transparência a lista de doadores e seus respectivos CPF's, assim como a quantia doada.

Deste modo, procurou-se analisar essa dinâmica específica tendo em conta os procedimentos demandados pela LGPD, investigando-se se estão em sintonia com as exigências e os requisitos legais, notadamente o consentimento, elemento fulcrar no tratamento de dados pessoais. Para tanto, fez-se oportuno realizar uma

digressão sobre o Direito Eleitoral e o funcionamento da Justiça Eleitoral.

Ainda com ressonâncias nessa esfera, verificou-se que o uso da biometria eleitoral para fins investigatórios permite uma análise ampla a respeito do tratamento dos dados pessoais pelo Poder Público, bem como das finalidades deste tratamento, discorrendo-se sobre a evolução legislativa, centrando-se em um caso concreto recente que permitiu digressionar a esse respeito. Por fim, reconhece-se que o presente trabalho não tem aptidão de abranger toda a matéria, mas visa trazer elementos para a sua compreensão global a partir de aplicações práticas, ilustrativas da importância e da atualidade deste tema.

REFERÊNCIAS BIBLIOGRÁFICAS

ARMANDO, Coronel. **Projeto de Lei da Câmara dos Deputados nº 1515, de 2022**. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/propostas-legislativas/2326300. Acesso em: 17 abr. 2023.

BATISTA, Anderson Röhe Fontão. PASSAPORTE COVID-19: risco e bioética na era da certificação digital. **Anais de Artigos Completos do VI CIDH**, Coimbra 2021 – Volume 7. *In*: César Augusto R. Nunes *et. al*. (orgs.). Campinas/Jundiaí, SP: Editora Brasílica/Edições Brasil, 2022.

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021.

BRASIL. [Código de Defesa do Consumidor (1990)]. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências (Código de Defesa do Consumidor). Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 abr. 2023.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**.
Brasília, DF: Presidência da República, [2023]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 abr. 2023.

BRASIL. [Lei das Eleições]. **Lei nº 9.504, de 30 de setembro de 1997**. Brasília, DF: Tribunal Superior Eleitoral, [2023]. Disponível em: https://www.tse.jus.br/legislacao/codigo-eleitoral/lei-das-eleicoes/lei-das-eleicoes-lei-nb0-9.504-de-30-de-setembro-de-1997. Acesso em: 28 jun. 2023.

BRASIL. [Lei de Acesso à Informação]. **Lei nº 12.527, de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 22 jun. 2023.

BRASIL. [Lei Geral de Proteção de Dados]. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 abr. 2023.

BRASIL. **Lei nº 13.444, de 11 de maio de 2017**. Dispõe sobre a Identificação Civil Nacional (ICN). Brasília, DF: Presidência da República, [2023]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm. Acesso em: 24 maio 2023.

BRASIL. Superior Tribunal de Justiça (Quarta Turma). **Recurso Especial n. 22.337/RS**. SERVIÇO DE PROTEÇÃO AO CRÉDITO. CANCELAMENTO DO REGISTRO. PRAZO (CINCO ANOS). O REGISTRO DE DADOS NO SPC DEVE SER CANCELADO APÓS CINCO ANOS. ART. 43, PARAGRAFO 1, DO CODIGO DE DEFESA DO CONSUMIDOR (LEI 8.078/90). Relator: Min. Ruy Rosado de Aguiar, 13 de fevereiro de 1995, Brasília, DF. Publicado no Diário da Justiça em 20 mar.1995, p. 6119. Disponível em: https://processo.stj.jus.br/processo/ita/documento/mediado/?num_registro=199200114466&dt_publicacao=20-03-1995&cod_tipo_documento=&formato=PDF. Acesso em: 25 abr. 2023.

BRASIL. Superior Tribunal de Justiça (Segunda Turma). **Agravo em Recurso Especial n. 2.130.619/SP**. PROCESSUAL CIVIL E ADMINISTRATIVO. INDENIZAÇÃO POR DANO MORAL. VAZAMENTO DE DADOS PESSOAIS. DADOS COMUNS E SENSÍVEIS. DANO MORAL PRESUMIDO. IMPOSSIBILIDADE. NECESSIDADE DE COMPROVAÇÃO DO DANO. Relator: Min. Francisco Falcão, 7 de março de 2023. Publicado no DJE em 10 mar.2023. Disponível em: https://scon.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=202201522622&dt_publicacao=10/03/2023.Acesso em: 05 abr. 2023.

BRASIL. Supremo Tribunal Federal. **Inquérito nº 4923**. Relator: Min. Alexandre de Moraes, 03 de fevereiro de 2023. Publicado no DJE em 09 de fevereiro de 2023, Brasília, DF. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/INQ4929AUTORIZAaOPARACONFERIMENTODEBIOMETRIA.pdf. Acesso em: 17 abr. 2023.

BRASIL. Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade nº 6.649 e Arguição de Descumprimento de Preceito Fundamental nº 695**. Relator: Min.Gilmar Mendes, 15 de setembro de 2022. Publicado no DJE nº 191 em: 26 de se tembro de 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?inci dente=5938693. Acesso em: 17 abr. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.607, de 17 de dezembro de 2019**; Dispõe sobre a arrecadação e os gastos de recursos por partidos políticos e candidatas ou candidatos e sobre a prestação de contas nas eleições. Publicada no DJE-TSE, nº 249, de 27.12.2019, p. 125-156, republicado no DJE-TSE, nº 165, de 19.8.2020, p. 105-147, republicada no DJE-TSE, nº 37, de 7.3.2022, p. 67-111 e republicada no DJE-TSE, nº 45, de 16.3.2022, p. 64-108. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-607-de-17-de-dezembro-de-2019. Acesso em: 23 abr. 2023.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.656, de 7 de outubro de 2021**. Dispõe sobre o acesso a dados pessoais constantes dos sistemas informatizados da Justiça Eleitoral (JE). Diário de Justiça Eletrônico (DJE) nº 190, Brasília, 15 de outubro de 2021, p. 90-95. Disponível em: https://sintse.tse.jus.br/documentos/2021/Out/15/diario-da-justica-eletronico-tse/resolucao-no-23-656-de-7-de-outubro-de-2021. Aceso em: 30 mar. 2023.

BROWN, Elizabeth Anne. DNA já pode ser retirado do ar. E isso preocupa. Tradução Renato Prelorentzou. **O Estado de S.Paulo** e **The New York Times**, Nova Iorque, EUA, ano 144, nº 47346, 4 jun. 2022. Caderno A Fundo, p. 6-7.

CARVALHO NETO, Tarcisio Vieira de. Transparência do processo eleitoral brasileiro. **Estudos eleitorais** (Tribunal Superior Eleitoral), Brasília, DF, vol. 1, n. 1, p. 9-27, maio/ago. 2016.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 2. p. 91-108, jul./dez. 2011.

FLEMING, Maria Cristina. LGPD: diferenças no tratamento de dados pessoais e dados pessoais sensíveis. **Conjur**, São Paulo, SP, 6 mar.2021. Disponível em: https://www.conjur.com.br/2021-mar-06/fleming-diferencas-tratamento-dados-pessoais-sensiveis. Acesso em: 10 abr. 2023.

GOMES, José Jairo. **Direito Eleitoral**. 19 ed. rev. atual. Barueri, SP: Atlas, 2023. *E-book*. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559775330/. Acesso em: 21 jul. 2023.

GROBÉRIO, Sandra do Carmo. MONITORA COVID-19: dever de disponibilizar dados pessoais sobre infecção em aplicativo e o direito à privacidade à luz da LGPD. **Anais de Artigos Completos do VI CIDH**, Coimbra, 2021, Volume 7. *In*: César Augusto R. Nunes *et. al*. (orgs.) [et al.] – Campinas/Jundiaí, SP: Editora Brasílica/Edições Brasil,

2022.

INTERNAUTAS pedem boicote à YPÊ após doações de donos a Bolsonaro. **Poder360**, 17 out.2022. Disponível em: https://www.poder360.com.br/eleicoes/internautas-pedem-boicote-a-ype-apos-doacoes-de-donos-a-bolsonaro/. Acesso em: 21 maio 2023.
LONGHI, João Victor Rozatti. **Responsabilidade civil e redes sociais**: retirada de conteúdo, perfis falsos, discurso de ódio e fake news. Indaiatuba, SP: Editora Foco, 2020.

NOVO juiz da lava jato doou R$ 13 para a campanha de Lula. **Poder360**, 17 fev. 2023. Disponível em: https://www.poder360.com.br/justica/novo-juiz-da-lava-jato-doou-r-13-para-a-campanha-de-lula/. Acesso em: 21 maio 2023.

OLIVEIRA, Bruno Ferreira de. Prestação de contas eleitorais e a não identificação de doadores do art. 28, § 12, d alei das eleições: análise da medida cautelar em ação direta de inconstitucionalidade nº 5.394/DF. **Estudos eleitorais** (Tribunal Superior Eleitoral), Brasília, DF, vol. 1, n. 1, p. 151-171, maio/ago. 2016.

RIO GRANDE DO SUL. Tribunal de Justiça (Décima Câmara Cível). **Apelação Cível nº 51393545820218210001**. APELAÇÃO CÍVEL. AÇÃO DECLARATÓRIA CUMULADA COM OBRIGAÇÃO DE FAZER E INDENIZAÇÃO POR DANOS MORAIS. VEICULAÇÃO DE INFORMAÇÕES EM CONSULTA DE CRÉDITO. AUSÊNCIA DE ILEGALIDADE DO REGISTRO. LGPD. Relator: Des. Jorge Alberto Schreiner Pestana, 23 fev.2023. Publicado no DJE em 27 fev. 2023. Disponível em: https://www.tjrs.jus.br/buscas/jurisprudencia/exibe_html.php. Acesso em: 17 mar.2023.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet? Tradução Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**. Rio de Janeiro, a. 4, n. 2, p. 1-8, jul.-dez./2015. Disponível em: <http://civilistica.com/por-que-e-necessaria-uma-carta-de-direitos-da-internet/>. Acesso em: 10 abr. 2023.

RODRIGUES, Ricardo Schneider; RUARO, Regina Linden. O serviço remunerado de conferência de dados por biometria à luz do direito fundamental à proteção de dados pessoais: a aplicação da lei nº 13.444/2017 pelo TSE. **Revista Jurídica Luso-Brasileira (RJLB)**, Lisboa, n.3, ano 7, p. 1291-1331, 2021.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra Sales. O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – lei 13.709/2018. *In*: BIONI, Bruno Ricardo (coord.). **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021. *E-book.* Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 02 abr. 2023.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**: uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13. ed. Porto Alegre: Livraria do Advogado, 2018.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. **Direitos Fundamentais & Justiça**, Belo Horizonte, MG, ano 14, n. 42, p. 179-218, jan./jun. 2020.

SCHREIBER, Anderson. **Novos paradigmas da responsabilidade civil**: da erosão dos filtros da reparação à diluição dos danos. 5. ed. São Paulo: Atlas, 2013.

SCRUTON, Roger. **O rosto de Deus**. Tradução Pedro Sette-Câmara. São Paulo: É Realizações, 2015.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth Maria. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Comentada Artigo por Artigo. São Paulo: Editora Saraiva, 2022. *Ebook*. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 30 mar. 2023.

UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados (RGPD).** Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 11 abr. 2023.

8. ASSÉDIO ELEITORAL NO AMBIENTE DE TRABALHO SOB A PERSPECTIVA DA LGPD: ANÁLISE JURISPRUDENCIAL APÓS ELEIÇÕES PRESIDENCIAIS NO BRASIL DE 2022

ELECTORAL HARASSMENT IN THE WORKPLACE UNDER THE PERSPECTIVE OF THE LGPD: JURISPRUDENTIAL ANALYSIS AFTER THE 2022 PRESIDENTIAL ELECTIONS IN BRAZIL

Plinio Gevezier Podolan[1]

https://doi.org/10.36592/9786554600712-08

SUMÀRIO

1. INTRODUÇÃO. 2. FUNDAMENTOS JURÍDICOS POSSÍVEIS PARA PROTEÇÃO EM FACE DO ASSÉDIO ELEITORAL. *2.1. Ofensa constitucional múltipla. 2.2. Violação de direitos humanos. 2.3. Direito ao meio ambiente de trabalho equilibrado. 2.4. LGPD: violação de dados sensíveis. 2.5. Crime eleitoral.* 3. ANÁLISE JURISPRUDENCIAL NO ÂMBITO DAS ELEIÇÕES PRESIDENCIAIS. 4. CONSIDERAÇÕES FINAIS

RESUMO

Considerando o assédio eleitoral no ambiente do trabalho como norte, em especial nas eleições presidenciais de 2022, o presente estudo objetiva fazer uma análise comparativa da fundamentação jurídica usada pelo Judiciário Trabalhista nas ações que versaram sobre esse tema. Num primeiro momento, valendo-se de uma pesquisa bibliográfica e documental, apresenta-se o que se compreende como arcabouçou transversal jurídico, dando ênfase, entre outros elementos, aos fundamentos previstos na Lei Geral de Proteção de Dados (LGPD), uma vez que a prática assediadora em questão afeta diversos aspectos da personalidade da correspondente vítima, para além do dano civil. Além disso, configura-se em prática criminosa, que alcança não apenas o indivíduo, mas também a sociedade, pois atentar contra o estado democrático de direito. Em seguida, valendo-se do método hipotético-dedutivo, assim como da comparação com a premissa jurídica apresentada, analisa-se uma amostragem de julgamentos de primeiro e segundo graus da Justiça do Trabalho para averiguar o alcance das fundamentações

[1] Doutorando em Direito pela PUCRS. Mestre em Direito pela UFMT. Especialista em Direitos Humanos pela PUCRS. Especialista em Direito do Trabalho e Processo do Trabalho pela PUCSP. Professor da Esmatra 23. Juiz do Trabalho.
E- mail: pliniopodolan@gmail.com. Currículo Lattes: http://lattes.cnpq.br/4634553096251386.

expostas, nos casos em que o assédio fora demonstrado. Conclui-se, por fim, que apesar de a Constituição brasileira ser usada como elemento comum nas fundamentações decisórias, em nenhuma dessas se viu referência à LGPD, sendo que essa ausência de alguns fundamentos legais influencia, sobremaneira, o valor indenizatório para fins de reparação extrapatrimonial.
Palavras-chave: assédio eleitoral; direitos humanos; ambiente do trabalho; LGPD; indenização.

ABSTRACT

Considering electoral harassment in the work environment as a guide, especially in the 2022 presidential elections, this study aims to make a comparative analysis of the legal basis used by the Labor Judiciary in actions that dealt with this topic. At first, using a bibliographical and documental research, it presents what is understood as a transversal legal framework, emphasizing, among other elements, the fundamentals foreseen in the General Data Protection Law (LGPD), since the harassing practice in question affects various aspects of the corresponding victim's personality, in addition to the civil damage. In addition, it constitutes a criminal practice, which reaches not only the individual, but also society, as it violates the democratic rule of law. Then, using the hypothetical-deductive method, as well as the comparison with the legal premise presented, a sample of judgments of the first and second degrees of the Labor Court is analyzed to verify the scope of the exposed grounds, in cases where harassment was demonstrated. Finally, it is concluded that although the Brazilian Constitution is used as a common element in the decision-making grounds, none of them saw reference to the LGPD, and this absence of some legal grounds greatly influences the indemnity value for reparation purposes.
Keywords: election harassment; human rights; work environment; LGPD; legal damages.

1. INTRODUÇÃO

O assédio eleitoral se apresenta como uma das formas de assédio moral e se configura quando o empregador, ou alguém que o represente, de forma intimidatória ou coativa, exige ou manipula, por ação direta ou indireta, o empregado a se filiar em partido ou a votar em candidato de sua preferência. Esse fenômeno acontece de várias maneiras, seja sob a forma de exigência direta, sob a possibilidade de conceder bônus ou vantagem financeira extracontratual, ou ainda, sob a forma de ameaça, prática que se revelou mais comum nas eleições brasileiras de 2022. Ameaça essa consistente na perda do emprego caso o candidato de preferência não ganhasse as eleições, imputando à escolha eleitoral do trabalhador uma

consequência negativa, ou ainda, a ideia de que o possível insucesso do seu negócio derivaria disso.

Como toda forma de assédio, o assédio eleitoral contamina o meio ambiente de trabalho, causando pressão psicológica e medo, desdobrando-se em doenças ou eventos psicossomáticos, como angústia, estresse, ansiedade e até depressão.

Ações indenizatórias por danos morais decorrentes desse tipo de assédio inundaram o Judiciário Trabalhista nas últimas eleições presidenciais de 2022, de modo que os juízes e as juízas do trabalho e os tribunais trabalhistas em geral precisaram analisar as demandas trazidas nesse cenário e, a partir das provas colhidas, avaliaram se as condutas praticadas eram abusivas, passíveis ou não de indenização.

O propósito do presente trabalho é, considerando uma amostragem de casos concretos, avaliar os fundamentos jurídicos usados pela magistratura trabalhista nos casos em que foi configurada a lesão ao direito de personalidade do trabalhador, a fim de averiguar eventual conexão com a proteção conferida pela Lei n.º 13.709/2018 – Lei Geral de Proteção de Dados (LGPD). Assim, a partir da metodologia hipotético-dedutiva, a pesquisa está calcada, inicialmente, na bibliografia apartada para esse desiderato, a fim de indicar um arcabouço teórico-jurídico de fundamentação protetiva e, na sequência, procede-se uma análise de decisões judiciais proferidas para realizar esse contraste entre a proteção multinível aqui declinada e aquela conferida na prática judicial trabalhista.

2. FUNDAMENTOS JURÍDICOS POSSÍVEIS PARA PROTEÇÃO EM FACE DO ASSÉDIO ELEITORAL

2.1. Ofensa constitucional múltipla

A Constituição brasileira, por si só, revela uma gama de direitos fundamentais mais que suficientes para embasar a proteção jurídica do trabalhador em face de eventual assédio eleitoral. Pode-se iniciar, por exemplo, por um de seus fundamentos republicanos, que pressupõe pluralismo político (art. 1º, V), o que, aliás, é base de todo estado democrático de direito. Tal pluralidade pressupõe a possibilidade de que

qualquer pessoa no Brasil se alinhe a um partido político, segundo sua convicção pessoal, ou ainda, sequer se identifique com qualquer dos 30 partidos oficialmente registrados no país[2].

Somado a isso, tem-se a liberdade de consciência, de crença, de convicção política ou filosófica (art. 5º, VI, VIII), todos esses que formam, entre si, um núcleo fundamental ao direito de autodeterminação, que se verá adiante, em tópico sobre a legislação afeta à proteção de dados.

No mesmo artigo 5º, não há como se olvidar o valor da liberdade que não só se reproduz explicitamente em seu *caput*, mas como é traduzido sob outras formas, a exemplo da redação dada ao inciso II, quando afirma que "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei". A relação imanente com o tema ora apreciado se revela à medida que a exigência de que um empregado vote em um determinado candidato da preferência do empregador não se insere dentro dos limites do poder diretivo deste. Não há, portanto, lei que determine que o empregado assim proceda. Pelo contrário, há lei que veda a conduta de conjurar votos pelo empregador, revelando-se, primariamente, abusiva e, quiçá, criminosa, como se demonstrará mais tarde.

Analisando-se em conjunto, o inciso XX, do art. 5º, embora refira-se à liberdade de associação, ele ratifica a vedação de compelir alguém a se associar, cuja redação se repete no também fundamental direito de filiação sindical previsto no art. 8º, V, da Constituição brasileira. Tal associação pode ser erigida ao patamar da associação político-partidária. Não se pode, portanto, compelir alguém a filiar-se em partido político ou constranger seu voto.

Tampouco se pode exigir do empregado a revelação de seu voto, seja porque há nisso violação direta do artigo 14 da Constituição brasileira, que assegura a qualquer cidadão o sigilo do voto, cujo objetivo, entre outros, é garantir-lhe autonomia na escolha de seu candidato e, ademais, configura-se em invasão da esfera da privacidade e da autodeterminação subjetiva, sendo oportuno adiantar que a convicção política foi tida como dado pessoal sensível, como previsto no art. 5º, II,

---

[2] BRASIL. Tribunal Superior Eleitoral. *Partidos Políticos registrados no TSE*. Disponível em: https://www.tse.jus.br/partidos/partidos-registrados-no-tse. Acesso em 16 ago. 2023.

da LGPD, cuja tutela também encontra proteção constitucional, em seu artigo 5º, inciso LXXIX.

Haverá quem possa alegar, e o aparte se faz desde logo, de que não haveria qualquer violação de direito ou conduta abusiva quando o empregador, em conversa com seu empregado, pede a esse que vote em alguém, expondo-lhe seus motivos, como se de uma mera conversa se tratasse. Esse discurso, contudo, ignora um contexto indisfarçável. O empregado, como se sabe, tal qual em outros contratos assimétricos, é tido presumivelmente hipossuficiente. Pesa sobre ele não só o poder diretivo do empregador, que deve exercê-lo dentro dos limites legais, mas também o temor reverencial, assim como a angústia de uma possível demissão num mercado de trabalho cada vez mais instável, com desemprego em massa causado por crises econômicas, pandemias e tecnologia. Não se trata, pois, de uma "mera conversa", despida de força coercitiva. Quando o empregador diz *gostaria que votasse em tal candidato pois será melhor para o país e, consequentemente para você*, acaba por incutir no trabalhador uma ideia de risco, de insegurança, quebrando a capacidade de autonomia do empregado e ferindo a sua liberdade em quem votar. À propósito, não há contrato de trabalho que possa estabelecer como obrigação imanente a fidelidade política ao empregador, pois, como dito alhures, ninguém pode ser compelido a associar-se politicamente.

Além disso, a relação de emprego, ou mesmo de trabalho, como gênero, possui como objeto a força de trabalho da pessoa contratada. Nesse sentido, historicamente, a jurisprudência foi assentando que condições pessoais dissociadas da capacidade laborativa não devem ser objeto de discriminação pelas empresas. Não se pode, por exemplo, deixar de contratar alguém em virtude de sua raça, sua etnia, sua crença religiosa, sua compleição física, entre outros fatores, sob pena de se praticar discriminação ou racismo, a depender da situação. A não contratação ou a dispensa, ou ameaça de dispensa do trabalho por convicção política insere-se na mesma análise da ofensa aos direitos de personalidade, passíveis, portanto, de indenizações extrapatrimoniais.

Decerto que, ao final deste trabalho, a análise se debruçará sobre casos em que os empregadores, dentro da amostragem sob escrutínio, usaram de artifícios implícitos ou explícitos para chantagear ou coagir os trabalhadores a eles

subordinados a votarem em um determinado candidato à presidência do país, quando então ficará mais claro, na prática, as formas como se dá a violação de tais direitos fundamentais.

2.2. Violação de direitos humanos

Além da proteção constitucional acima descrita, não se pode ignorar a exigência do controle de convencionalidade na subsunção e interpretação jurídica, conforme previsto pelos arts. 1º e 2º da Convenção Americana sobre Direitos Humanos, exercício a que a magistratura está obrigada a fazer, sobretudo quando se tratam de convenções internacionais sobre direitos humanos como a liberdade de convicção política. Sobre esse tema, inclusive, o Conselho Nacional de Justiça publicou a Resolução n.º 364/2021 que orienta juízes e juízas a adotarem as decisões e deliberações da Corte Interamericana de Direitos Humanos, dando relevo às decisões e normas internacionais[3].

Assim, citam-se, apenas de início, a Declaração Universal dos Direitos Humanos (arts. 1º, 2º, 7º, 12, 14, 18 e 19), o Pacto Internacional de Direitos Civis e Políticos (art. 25) e Convenção Americana de Direitos Humanos – Pacto de San José da Costa Rica (art. 1º), aos quais se submete o Brasil e que proíbem qualquer discriminação ou perseguição por convicção política.

Em matéria trabalhista, como se sabe, as convenções da Organização Internacional do Trabalho (OIT), que tratam sobre direitos sociais, são consideradas tratados de direitos humanos, sendo, historicamente, os primeiros direitos a serem reconhecidos em âmbito internacional, a exemplo da Declaração de Filadélfia, de 1944 e de outros tratados internacionais[4]. Nesse sentido, como se adiantou no tópico anterior, ainda que não sejam equivalentes a emendas constitucionais, em virtude da não superação de um requisito formal, qual seja, a aprovação por mais de dois terços

[3] CARVALHO, Felipe Rodolfo de; PODOLAN, Plínio Gevezier. A reforma trabalhista e a ofensa ao direito humano de livre acesso à justiça: uma análise do duplo controle de verticalidade. In *Revista Magister de Direito do Trabalho.* N. 112, p. 51-76, Porto Alegre: Magister, 2023, p. 67.

[4] MAZZUOLI, Valério de Oliveira; MARANHÃO, Ney; AZEVEDO NETO, Platon Teixeira de. Direitos Humanos e Direito Internacional Público: considerações à luz da tutela jurídico-internacional do ser humano que trabalha. *In: Revista de Direito do Trabalho e Seguridade Social*. V. 216, p. 239-272. São Paulo: Ed. RT, 2021, p. 7.

dos membros de cada casa do Congresso Nacional, o Supremo Tribunal Federal consolidou a interpretação de que tais normas têm status de supralegalidade, conforme se depreende dos julgamentos do HC n.º 87.585/TO e do RE n.º 466.343/SP.

Ciente disso, é relevante destacar a Convenção n. º 111 da OIT, ratificada pelo Brasil desde 26 de novembro de 1965, e que conceitua discriminação como "toda distinção, exclusão ou preferência fundada na raça, cor, sexo, religião, opinião política, ascendência nacional ou origem social, que tenha por efeito destruir ou alterar a igualdade de oportunidade ou de tratamento em matéria de emprego ou profissão" (art. 1º, a).

Assim, se em alguma medida, o trabalhador sentir sua autonomia de determinação política tolhida em virtude de ameaça - explícita ou não - ou de coação, um direito humano seu está sendo violado, revelando a gravidade da lesão e, por conseguinte, influindo na análise do dano extrapatrimonial. Repita-se que mesmo o mero exercício de persuasão, quando realizado no ambiente do trabalho e em virtude desse, pode se configurar em assédio, sobretudo em virtude da assimetria contratual que se revela na maior parte dos casos, o que gera a presunção de hipossuficiência do trabalhador.

2.3. Direito ao meio ambiente de trabalho equilibrado

Como mencionado no início deste trabalho, o assédio, em suas diversas formas, contamina o meio ambiente de trabalho[5], trazendo um contexto de insalubridade psicológica. Essa percepção não raramente passa despercebida em tais situações, as quais são normalmente analisadas tão somente sob a perspectiva individual da vítima da agressão psicológica. Contudo, o meio ambiente

---

[5] Sugere-se a adoção do conceito proposto por Maranhão, para quem o "meio ambiente do trabalho é a resultante da interação sistêmica de fatores naturais, técnicos e psicológicos ligados às condições de trabalho, à organização do trabalho e às relações interpessoais que condiciona a segurança e a saúde física e mental do ser humano exposto a qualquer contexto jurídico-laborativo" (MARANHÃO, Ney. Meio ambiente do trabalho: descrição jurídico-conceitual. In *Revista Direitos, Trabalho, e Política Social.* V. 2, n. 3, p. 80-117, Cuiabá, jul./dez. 2016, p. 112).

desequilibrado afeta a todos que nele convivem ou dele dependem, incluindo-se, é claro, o meio ambiente do trabalho.

A tutela ao meio ambiente saudável e equilibrado é também um direito assegurado ao trabalhador por meio do artigo 7º da Constituição brasileira quando convoca, em seu inciso XXII, a reduzir os riscos inerentes ao trabalho, por meio de normas de saúde e segurança. Não se trata aqui apenas da prevenção aos riscos a acidentes de trabalho com infortúnio que lesa o corpo do trabalhador, mas também abrange a sua saúde mental que, a depender da gravidade da lesão, pode levá-lo à morte.

Nesse sentido, valendo-se dos mesmos argumentos sobre a natureza de supralegalidade dos tratados internacionais que versem sobre direitos humanos, a Convenção n.º 155 da OIT, que trata da segurança e saúde dos trabalhadores, ratificada pelo Brasil em 18 de maio de 1992, afirma que "o termo saúde, com relação ao trabalho, abrange não só a ausência de afecções ou doenças, mas também os elementos físicos e mentais que afetam a saúde" (art. 3º, e). Para corroborar tais argumento, no âmbito legal, a Lei n.º 8.080/1990 afirma, em seu art. 2º, que "a saúde é um direito fundamental do ser humano" e que esse direito compreende a garantia de condições de bem-estar físico, mental e social (art. 3º, parágrafo único). Como se vê, a dimensão psicossocial de bem-estar integra o conceito e, por conseguinte, o direito à saúde em qualquer esfera social, inclusive no meio ambiente laboral.

Nesse sentido, o ato de amedrontar o trabalhador quanto à sua permanência ou não em seu vínculo de emprego, por razões políticas, gera nesse indivíduo angústia e temor, provoca a ruptura de sua autonomia, coagindo-o a se submeter, porque subordinado é, aos interesses de seu empregador, com os quais, eventualmente, não comunga. Aliás, o medo é um instrumento poderoso de manipulação, pois em sua oposição, o ser humano foge dele em busca de segurança. Porém, nem sempre o medo é real, ele pode ser incutido, forjado, baseado em desinformação ou, como ocorre numa relação de poder, no desejo de que o poder seja mantido como está. Assim, se inocula medo para garantir subserviência. Adorno[6], por exemplo, refere-se ao medo para ilustrar como os nazistas o utilizaram

---

[6] ADORNO, Theodor W. *Educação e emancipação*. Tradução de Wolfgang Leo Maar. 3. ed. São Paulo: Paz e Terra, 2003, p. 124.

a fim de afetar a capacidade de reflexão e de autodeterminação, isto é, mitigando qualquer possibilidade de reação da pessoa oprimida, em situação de vulnerabilidade.

Não há dúvidas de que a análise de qualquer modalidade de assédio passa, necessariamente, pela tutela da garantia de um meio ambiente de trabalho equilibrado. Mas não só. No caso do assédio eleitoral, há um elemento adicional que deve ser levado em consideração. Com o advento da LGPD e com a inclusão do inciso LXXIX no art. 5º, da Constituição brasileira, a partir da EC n.º 115/2022, outro viés protetivo merece ser destacado e que tem sido negligenciado pelo Judiciário trabalhista. A relevância de se colocar em foco essa proteção multinível afeta não só o seu alcance formal, mas também a sua concretude, uma vez que para análise de eventual quantia indenizatória-reparatória, o juiz e a juíza devem levar em consideração a extensão do dano, conforme preceitua o art. 944 do Código Civil e a natureza jurídica do bem tutelado, como afirma o artigo 223-G, da CLT, dentre outros critérios. Tendo sua personalidade atingida por vários fatores tutelados pela lei e, nesse caso, por violação de direitos humanos e fundamentais, a conduta abusiva, quando demonstrada, revela-se gravíssima.

2.4. LGPD: violação de dados sensíveis

Esse item, portanto, propõe-se a destacar que eventual assédio eleitoral cometido em face de um empregado não só revela uma prática que ofende o meio ambiente do trabalho, mas também viola o sistema protetivo de seus dados pessoais, sobretudo dados sensíveis.

O art. 2º da LGPD disciplina os fundamentos que sustentam essa proteção, dentre os quais, citam-se o respeito à privacidade (inciso I), a autodeterminação informativa (inciso II), a inviolabilidade da intimidade (IV) e, por fim, mas certamente o mais importante, o respeito aos direitos humanos, ao livre desenvolvimento da personalidade, à dignidade e ao exercício da cidadania pelas pessoas naturais (inciso VII)[7].

[7] "Reafirma-se a imprescindibilidade do princípio da responsabilidade quando se trata dessa temática. [...] (N)o meio ambiente digital/virtual, em específico no que afeta ao tratamento de dados

Não pode o empregador, portanto, à despeito de considerar sua opinião política mais abalizada ou que supostamente beneficiará seu estilo de vida, valer-se de seu poder diretivo e da relação jurídica subordinada do seu empregado para, por exemplo, invadir sua intimidade, a fim de conhecer qual sua pretensão de voto, o que, como dito antes, fere o direito ao sigilo previsto no artigo 14 da Constituição brasileira ou, ainda, tentar influenciá-lo de modo parcial, obscuro ou intimidatório, afetando sua autodeterminação informativa. Quando, portanto, o trabalhador tem a sua liberdade tolhida ou mitigada, liberdade essa aqui vista sob a perspectiva da sua personalidade e de como ela se expressa no mundo, tem-se, ao mesmo tempo, sua dignidade ferida.

Prosseguindo, o art. 5º, II, da LGPD inclui a opinião política como dado pessoal sensível, conferindo-lhe, portanto, um nível de proteção ainda maior do que o dado pessoal comum. E, nesse caso, havendo violação pelo empregador, em razão do exercício de sua atividade, causando algum dano moral ao titular do dado, no caso, o trabalhador, ele deverá ser responsabilizado civilmente por isso, também sob essa perspectiva, como preceitua o art. 42 da LGPD.

Ainda sobre a LGPD, um último destaque merece ser realizado, sobretudo para os que atuam na seara trabalhista. Na análise das decisões que foram usadas como amostragem neste trabalho, as quais serão apresentadas em tópico próprio, notou-se que os juízes e as juízas do trabalho valeram-se, nas situações de assédio eleitoral, da típica distribuição do ônus probatório prevista no artigo 818, da CLT, imputando ao trabalhador tal ônus por considerar que se trata de fato constitutivo do seu direito de reparação. Contudo, o art. 42, § 1º da LGPD, valendo-se da premissa de hipossuficiência do titular dos dados, a mesma premissa que é usada na seara consumerista ou trabalhista, diz que "o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação,

---

sensíveis, torna-se igualmente elementar a aplicação dos princípios da precaução e da prevenção como pilares de uma constelação jurídica que tem como vetor primordial a proteção da dignidade da pessoa humana, dentro e fora do ambiente digital". Cf. SARLET, Gabrielle Bezzera Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) – L.13.709/2018. In *Revista de direitos fundamentais e democracia*, v. 26, n. 2, p. 81-106, mai./ago. 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em: 20 ago. 2023, p. 85.

houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa". Aqui, portanto, advoga-se a tese de que, no caso de assédio eleitoral, considerando que a convicção política é um dado pessoal sensível, havendo verossimilhança da alegação feita pelo trabalhador, o juiz ou a juíza que conduzem o caso, poderão inverter (ou distribuir) o ônus, atribuindo ao empregador o ônus da prova de que não cometeu o alegado assédio.

Situação semelhante já vem sendo aplicada há algum tempo nos casos, por exemplo de assédio sexual, baseando-se nas mesmas premissas: hipossuficiência da vítima do assédio e dificuldade ou onerosidade extrema da produção de prova. Tal distribuição do ônus da prova foi, inclusive, recomendada pelo Protocolo para julgamento com perspectiva de gênero publicado pelo Conselho Nacional de Justiça[8].

Percorrido esse caminho, não bastasse todas as infrações de natureza civil acima expostas, o assédio eleitoral pode, ainda, configurar-se em crime.

2.5. Crime eleitoral

A começar pelo Código Penal, o art. 359-P considera crime "restringir, impedir ou dificultar, com emprego de violência física, sexual ou psicológica, o exercício de direitos políticos a qualquer pessoa". Nesse passo, ao coagir alguém psicologicamente a votar em um determinado candidato, tem-se certamente configurado o tipo penal em análise, impedindo-se o pleno exercício dos direitos políticos. Ainda, de forma mais específica, o Código Eleitoral considera crime eleitoral "usar de violência ou grave ameaça para coagir alguém a votar, ou não votar, em determinado candidato ou partido, ainda que os fins visados não sejam conseguidos" (art. 301), com previsão de pena de reclusão de até quatro anos e multa.

Não há dúvidas, portanto, seja sob a perspectiva civil, seja penal, que a conduta do assédio eleitoral é antijurídica, devendo ser erradicada do meio ambiente

---

[8] BRASIL. Conselho Nacional de Justiça. *Protocolo para julgamento com perspectiva de gênero.* Grupo de Trabalho instituído pela Portaria CNJ n.º 27, de 2 de fevereiro de 2021. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2021/10/protocolo-18-10-2021-final.pdf. Acesso em 20 ago. 2023, p. 109.

laboral e, quando manifestada, ter seus efeitos deletérios ressarcidos e punidos pelo agente coator. Como se evidencia, para além das violações aos direitos de personalidade, na esfera civil, gerando danos morais, há, por parte do empregador assediador, o cometimento de crime. Assim, em que pese as instâncias trabalhista e criminal serem autônomas entre si, é dever do magistrado ou da magistrada trabalhista, ao concluir pela ocorrência de assédio eleitoral, oficiar à autoridade policial competente, ao Ministério Público do Trabalho e ao Ministério Público acerca do ato praticado a fim de que investiguem o ilícito penal praticado e adotem as providências cabíveis.

3. ANÁLISE JURISPRUDENCIAL NO ÂMBITO DAS ELEIÇÕES PRESIDENCIAIS

Antes de se ingressar na análise da amostragem de decisões e julgados selecionados para o presente trabalho, intenta-se dissipar, desde logo, qualquer discussão sobre a materialidade e competência acerca da análise de violação desse dado sensível. Visto sob a perspectiva exclusiva da LGPD, muito provavelmente assentar-se-ia a competência na Justiça Comum, para analisar eventual dano de natureza civil decorrente dessa violação. Contudo, ao ser praticada em virtude do contrato de trabalho existente, tem-se a vinculação dos arts. 114, I e IX, da Constituição brasileira, sendo, portanto, da Justiça do Trabalho a competência para análise desse dano e o seu alcance para fins indenizatórios. Ainda que sua natureza seja um dano civil, que afeta, por exemplo, os direitos de personalidade, sua ocorrência no curso da relação de trabalho ou em virtude dela, vincula tal competência à Justiça especializada, tal como ocorre em outras violações de natureza civil que tenham sido praticadas no decorrer do contrato, a exemplo das indenizações por acidentes laborais ou por assédios em geral.

É imperioso, portanto, que o judiciário trabalhista note que há uma lesão múltipla a um direito de personalidade e também ao direito fundamental de proteção de dados, o que revela sua gravidade, a qual deve ser levada em consideração no momento da avaliação quantitativa do dano, em especial, o extrapatrimonial.

Sobre o assunto, o Ministério Público do Trabalho (MPT), ao tempo das eleições de 2022, tanto no primeiro como no segundo turno, merecendo destaque

aqui as eleições para o cargo mais alto do Poder Executivo, compilou todas as denúncias recebidas e produziu um relatório para mapear a ocorrência de assédio eleitoral. Nesse relatório, o MPT identificou um número expressivo de denúncias, concentradas nas regiões sul e sudeste:

> A grande maioria das condutas ilícitas denunciadas envolveram o pleito eleitoral relacionado à Presidência da República. Após o primeiro turno das eleições, o número de denúncias se intensificou: até o dia 03.10.2022, o número total de denúncias era 68 e o de empresas investigadas 52, enquanto, em 29.10.2022, os números saltaram para 2.360 denúncias e 1.808 empresas investigadas [...]. O ápice do número de denúncias registradas foi de 265 no dia 28 de outubro de 2022. A região com o maior número de denúncias até o primeiro turno era a Região Sul. O quadro se modificou após o dia 3.10.2022 em razão do expressivo número de denúncias e de empresas investigadas na Região Sudeste, com destaque para os Estados de Minas Gerais e São Paulo" (Brasil, MPT, 2022, p. 7).

Como se denota, foi muito expressivo o número de denúncias de assédio eleitoral formalizadas perante o MPT, sem considerar que há um potencial número de subnotificações e, em outros casos, trabalhadores que vindicaram direta e individualmente a tutela da jurisdição estatal, sem a mediação do órgão ministerial.

Esclarece-se que os exemplos que foram colhidos não são exaurientes. A amostragem serve, sobretudo, para ilustrar o *modus operandi* do assédio eleitoral e, em seguida, os fundamentos jurídicos usados nos julgamentos a fim de, como se disse, fazer um contraste com os elementos trazidos no item anterior.

Os primeiros exemplos a seguir citados cingem-se a decisões liminares que foram apreciadas em caráter de urgência nas vésperas dos dias de votação, a fim de evitar impedimento do exercício livre de voto, com seu caráter sigiloso.

Segundo o que se apurou no Inquérito Civil n.º 000595.2022.23.000/9, depois convertido na ACPCiv n.º 0000259-03.2022.5.23.0052, no município de Nova Olímpia/MT, no dia 19 de outubro, foi realizada uma reunião em que os empregados foram coagidos a votar em determinado candidato à Presidência. Em vídeo divulgado, é possível verificar uma empresária alertando sobre os riscos decorrentes de uma possível vitória do concorrente, sendo que um deles atingiria diretamente os

trabalhadores, provocando a perda de empregos. Na gravação, a pessoa aparece vestida com as cores da bandeira do país e com camiseta com a mensagem "Movimento Brasil".

O segundo caso, na ACPCiv n.º 0000639-55.2022.5.23.0107, no município de Poconé/MT, em 27 de outubro de 2022, a empregadora narrou que conversou com funcionários contrários ao candidato à reeleição de sua preferência para tentar *fazer a cabeça deles*, concluindo que o país vai continuar a melhorar se o político pelo qual manifestou seu favoritismo vencer as eleições. Ao final, externou, na entrevista, a opinião de que empregadores, por ajudarem as pessoas mais necessitadas, têm o direito de exigir o voto no candidato de sua preferência.

Revela-se uma conduta absolutamente abusiva. A empregadora, confessa de sua atitude assediadora, assim o fez por compreender que ao "ajudar" pessoas mais necessitadas ela tem o direito de exigir-lhes o voto em seu candidato, revelando-se a velha e não tão esquecida prática do voto de cabresto[9].

Outro ponto que chama a atenção é a ideia de que ao empregar alguém, a empresa estaria fazendo uma "caridade", esquecendo-se de que se trata de uma relação de natureza contratual, onde o trabalhador dispõe de sua força de trabalho, em troca de salário, para que ela, empregadora, obtenha lucro. Ou ela conseguiria dar continuidade a sua atividade econômica sem a mão-de-obra então contratada? Seu descolamento da realidade faz nascer dentro de si a consciência de um potencial direito que ela considera exigível do outro, no caso, do empregado, à despeito de sua personalidade, nesse aspecto, não ser objeto do contrato de trabalho. Nos dois casos acima citados, a Justiça do Trabalhou de primeiro grau deferiu a liminar a fim de coibir o assédio, determinando que os empregadores se abstivessem reiterar essas condutas.

---

[9] "Daí surgiu o termo "voto de cabresto" ou de "curral", justamente pelo controle da votação dos eleitores pertencentes a determinado cercado eleitoral chefiado por um coronel. Pelo voto de cabresto ou de curral, o povo recebia a cédula eleitoral já preenchida, com o voto marcado no candidato indicado, sendo este o ápice do coronelismo no Brasil, um País com mentalidade atrasada já para aquela época". Cf. CAMARA, Amanda Paoleli. Coronelismo nas eleições atuais: o protagonismo perigoso do assédio eleitoral no ambiente de trabalho. *In: Revista Economia e Globalização.* Publicado em 20 dez. 2022. Disponível em: http://revistadedireito.catolicasc.org.br/index.php/revistadedireito/article/view/35. Acesso em 19 ago. 2023, p. 7.

Prosseguindo, nos autos da Ação Trabalhista n.º 0000665-14.2022.5.23.0023, que tramita no Tribunal Regional do Trabalho da 23ª Região, outro caso ocorreu, dessa vez em Rondonópolis/MT. No dia 26 de outubro de 2022, foram apresentados áudios onde constam diversas ameaças caso o candidato da preferência do empregador não fosse eleito. Nesses áudios constataram-se intimidações que vão desde demissão em massa, substituição dos empregados por maquinário, fim do pagamento de bônus, entre outros. "Espero que os funcionários nossos pensem no patrão, né. Não pense só em trabalhar, tem que vestir a camisa"[10], diz trecho do áudio atribuído ao representante da empresa, reconhecido como patrão da fazenda. Assim como o exemplo anteriormente citado, isso configura uma ameaça ao estilo cabresto. Os trabalhadores são considerados como sua propriedade e, como tal, devem seguir suas ordens, as quais extrapolam os limites do poder diretivo dentro do contrato de trabalho[11]. Nesse último caso, a decisão liminar fixou multa em virtude da ameaça de demissão em massa, além de coibir a repetição da conduta criminosa.

Decerto que as decisões liminares, ainda que possam surtir um efeito pedagógico, não são impeditivas de que o empregador, desgostoso com a eventual convicção política de seu empregado, o demita, sem justa causa, uma vez que a dispensa arbitrária, da qual o empregado deveria estar protegido, conforme previsto no artigo 7º, I, da Constituição brasileira, não foi regulamentada pelo Legislativo e tampouco teve essa omissão corrigida pelo Judiciário[12]. Assim, salvo comprovação inequívoca de que a demissão se deu por essa razão, qual seja, a convicção política do empregado, não haveria óbice para a demissão arbitrária. Ainda assim, caso fosse

---

[10] BRASIL. Ministério Público do Trabalho. *Assédio Eleitoral. Eleições 2022*: Relatório de atividades. Publicado em novembro de 2022.

[11] "Essas violações passam pela deficiência de uma verdadeira consciência constitucional, fruto do particularismo, da aversão ao formalismo público, fazendo-se da atuação, que deveria ser republicana, muitas vezes, mera extensão da conduta privada, como se estivesse agindo no âmbito familiar ou da sua propriedade". Cf. FELICIANO, Guilherme Guimarães; CONFORTI, Luciana Paula. Sobre o assédio eleitoral no Direito do Trabalho: as novas veredas do velho coronelismo à brasileira. In *Revista Direito UNIFACS – Debate Virtual,* n. 274, 2023. Disponível em: https://revistas.unifacs.br/index.php/redu/article/view/8166/4805. Acesso em 25 ago. 2023, p. 10.

[12] O Legislativo brasileiro jamais publicou a lei complementar referida no art. 7º, I, da Constituição federal. A Convenção da OIT n.º 158 que trata sobre esse assunto e suprimiria a omissão em análise, embora tivesse sido ratificada pelo Brasil, foi denunciada por decreto unilateral do Presidente da República em 1996, razão por que se ingressou com a ADI 1625, em 1997, a qual, até hoje, não foi definitivamente julgada pelo STF.

provada a causa discriminatória da demissão, essa demandaria, no máximo, uma indenização de natureza civil em virtude de sua abusividade, mas não confere qualquer proteção à manutenção do emprego daquele trabalhador.

Por ser ainda muito recente, considerando-se o lapso temporal dos processos judiciais, não são numerosos os casos de assédio eleitoral que tenham ascendido ao grau revisor, sendo mais expressivos os casos julgados no primeiro grau. Porém, traz-se um exemplo julgado pelo Tribunal Regional do Trabalho da 4ª Região (RS), em que o trabalhador aduziu que o empregador expôs vídeos, nas eleições de 2018, dizendo que votassem em determinado candidato e que, se votassem no outro candidato, seriam demitidos. Segundo as provas orais colhidas, primeiro e segundo graus convenceram-se de que houve reuniões com o intuito de direcionar os empregados para a escolha eleitoral da empresa, sendo que duas testemunhas foram enfáticas ao confirma que se não votassem no candidato Bolsonaro seriam demitidos ou que os seus empregos "estariam em risco":

> INDENIZAÇÃO POR DANOS MORAIS. ASSÉDIO ELEITORAL. A Constituição Federal de 1988 protege a intimidade, a vida privada, a autodeterminação e a liberdade de consciência e manifestação do pensamento (art. 5°, caput, incisos II, IV, VI, IX, X, CF/88), sendo vedado que uma pessoa seja privada de seus direitos em razão de convicção política (art. 5°, VIII, CF/88). Ainda, no âmbito do direito do trabalho, ninguém pode sofrer discriminação em razão de opinião política, nos termos dos arts. 3°, 5°, XLI e 7°, XXX, XXXI, da CF/88 e Lei 9.029/95. Nesse sentido, tem-se que a tentativa de ingerência sobre o voto dos trabalhadores atenta contra o livre exercício dos direitos políticos e configura assédio eleitoral, representando abuso do poder diretivo da empresa. É o que ocorre no caso em análise, em que a prova dos autos confirma que os trabalhadores foram constrangidos pela reclamada a participar de reunião com o objetivo de direcionar sua escolha eleitoral. Dessa forma, resta caracterizado o dano moral indenizável. Recurso da reclamada desprovido[13].

[13] BRASIL. Tribunal Regional do Trabalho da 4ª Região. *ROT 0020964-33.2019.5.04.0124*. Relator André Reverbel Fernandes. Publicado em 08 mar. 2023. Disponível em: https://pesquisatextual.trt4.jus.br/pesquisas/rest/download/acordao/pje/uOSrE2htPJo6HyHeoSh0rQ. Acesso em 19 ago. 2023.

Como se verifica, o julgamento valeu-se do conjunto de direitos fundamentais que garantem a intimidade, a liberdade de consciência e de convicção política. Importante dizer que embora haja referência explícita à autodeterminação, não houve menção à LGPD como fundamento legal. Ainda, a Lei n. 9.029/95, que veda tratamento discriminatório no ambiente de trabalho, foi considerada como fundamento da decisão, o que igualmente poderia ser depreendido dos tratados internacionais de direitos humanos outrora citados, que possuem *status* de supralegalidade.

É relevante registrar que, para fins indenizatórios, tanto a juíza sentenciante de primeiro grau como a turma revisora arbitraram igual valor a título de danos morais, R$ 10.000,00 (dez mil reais), o que fora usado como parâmetro em outros casos semelhantes. Contudo, dada a extensão do dano, representada pelo conjunto de direitos fundamentais e humanos que são lesados, associada ao fato de que se trata de conduta criminosa, defende-se que o valor arbitrado está aquém daquele que imprimiria, para além do efeito reparatório, um efeito pedagógico, com o intuito de inibir a reiteração de condutas como essa pelo empregador assediador.

Apenas como ilustração, traz-se o julgamento do Ag-AIRR-2451-06.2016.5.12.0025 pelo Tribunal Superior do Trabalho (TST), em 27 de abril de 2022, de relatoria do Ministro Cláudio Brandão. Nesse caso, registra-se que não há, pela própria competência do Tribunal Superior, revisão de provas, não tendo sido reconhecida a transcendência da causa. Porém, da sua descrição e dos trechos transcritos no acórdão, tem-se que se tratou de caso de assédio eleitoral cabalmente demonstrado pelas provas produzidas no primeiro grau, configurando-se coação aos empregados, "em violação aos direitos fundamentais relativos à intimidade, igualdade e liberdade política"[14]. Entretanto, nesse caso, o valor indenizável por danos morais foi arbitrado em R$ 1.000,00 (mil reais), o que certamente não atende à expectativa reparatória adequada, repita-se, pelo conjunto de violações que foram perpetradas, de extrema gravidade.

---

[14] BRASIL. Tribunal Superior do Trabalho. Ag-AIRR-2451-06.2016.5.12.0025. Relator Min. Cláudio Brandão. Publicado em 27 abr. 2022. Disponível em https://jurisprudencia-backend2.tst.jus.br/rest/documentos/23df1e835b6c06b3b0e55e7eade3a32b. Acesso em 19 ago. 2023.

Agora, em situação ocorrida em Santa Catarina, analisada nos autos ROT n.º 0000190-47.2020.5.12.0019 do TRT da 12ª Região, a sentença sintetizou que:

> [...] A partir de fevereiro de 2018, a ré obrigou, sob pena de demissão, o uso de uma camiseta com as cores e slogan da campanha política do atual Presidente da República, e que foi implementada como uniforme; a gerente da loja transmitia aos empregados as "lives" do proprietário da ré, Sr. Luciano Hang, que ameaçava de demissão aqueles que não votassem em seu candidato à presidência[15].

A empresa fora condenada em primeiro grau a pagar uma indenização por dano moral no importe de R$ 10.000,00. Em recurso, a 5ª Câmara do TRT da 12ª Região decidiu pela manutenção da sentença, sob os seguintes fundamentos:

> ASSÉDIO MORAL. DIRECIONAMENTO DO VOTO EM ELEIÇÃO PRESIDENCIAL. VIOLAÇÃO AO LIVRE EXERCÍCIO DA CIDADANIA E À LIBERDADE DE CONVICÇÃO POLÍTICA. INDENIZAÇÃO DEVIDA. O discurso alarmista dirigido pelo proprietário da empresa aos seus empregados de fechamento de lojas e perda de empregos em caso de vitória de candidato à eleição presidencial diferente daquele que apoia constitui evidente conduta assediadora, em nítida afronta ao livre exercício da cidadania e à liberdade de convicção filosófica e política (art. 5º, VI e VIII, da CRFB/88)[16].

Como se denota, a fundamentação jurídica cingiu-se, mais uma vez, à liberdade de convicção filosófica, o que, como fora dito antes, é suficiente para embasar a condenação, mas não traz a totalidade de violações que decorre dessa conduta abusiva e ilegal, mantendo-se o *quantum* indenizatório no mesmo patamar de outros tribunais.

---

[15] BRASIL, Tribunal Regional do Trabalho da 12ª Região, *ROT 0000190-47.2020.5.12.0019,* Relatora Ligia Maria Teixeira Gouvea, Publicado em 20 abr. 2022. Disponível em: https://pje.trt12.jus.br/consultaprocessual/detalhe-processo/0000190-47.2020.5.12.0019. Acesso em 19 ago. 2023.

[16] *Ibidem*.

Também em Santa Catarina, na Vara do Trabalho de Mafra, a juíza de primeiro grau, Izabel Maria Amorim Lisboa, analisando caso de assédio eleitoral, assim decidiu, após convencer-se de que as provas eram hábeis a prova-lo:

> [...] A prática da ré de divulgar nota interna condicionando a viabilidade e prosperidade do negócio e, de forma velada, a manutenção de todos os empregos ao resultado da disputa eleitoral, visou infundir no autor indiscutível pressão para votar no candidato apresentado como melhor opção por sua empregadora. Ocorre, todavia, que é do(a) empregador(a) a responsabilidade pelos riscos do empreendimento econômico (art. 2º da CLT), de modo que o sucesso ou insucesso do negócio não pode ser atribuído ou dependente da opção política de seus empregados. Não se discute que os sócios de qualquer empreendimento empresarial, como todo cidadão, têm constitucionalmente assegurados o direito à liberdade de expressão e de opinião política, podendo declarar livremente suas preferências ou apoiar candidatos de sua escolha. Contudo, isso não lhes confere o direito de utilizar de forma abusiva dos poderes econômico e diretivo que detêm no âmbito da(s) pessoa(s) jurídica(s) de que são proprietários, utilizando-os para coagir ou induzir o voto de seus empregados para um candidato, partido ou orientação política específica. Nesse contexto, a atitude patronal representou ataque a direitos extrapatrimoniais do autor, em especial do livre exercício da cidadania e da liberdade de convicção filosófica e política (art. 5º, VI e VIII, da Constituição Federal)[17].

Como se denota, a juíza considerou abusiva a conduta do empregador e, além dos fundamentos constitucionais mais usuais, acrescentou que, em virtude da assunção dos riscos do negócio, a alteridade do empregador prevista no artigo 2º da CLT, ele não pode condicionar a manutenção do sucesso do seu negócio à convicção política do trabalhador. Para esse caso, decidiu-se pela indenização no valor de R$ 5.000,00 (cinco mil reais), o que, mais uma vez, revelou não considerar, na prática, uma conduta de alta gravidade a ponto de exigir da empresa uma indenização maior.

---

[17] BRASIL. Vara do Trabalho de Mafra/SC. *ATOrd 0001324-47.2022.5.12.0017*. Juíza Izabel Maria Amorim Lisboa. Publicado em 27 jul. 2023.

Num outro exemplo recente, julgado pela Juíza Maria Iris Diogenes Bezerra, na 4ª Vara do Trabalho de Campina Grande/PB, essa também se convenceu, pelas provas produzidas, da ocorrência de assédio moral. Da análise das provas, concluiu:

> Os vídeos juntados pela reclamante evidenciam a situação por ela vivida, a coação eleitoral, no sentido de que declarassem o voto, quando o empregado determina que quem votasse em Jair Bolsonaro levantasse a mão, tendo apenas a reclamante ficado sem levantar as mãos, e o empregador condiciona a manutenção do vínculo de emprego ao voto em candidato de sua preferência[18].

Na fundamentação jurídica, a juíza cingiu-se ao artigo 5º, X, da Constituição federal e, ainda, dos artigos 186, 187 e 927 do Código Civil para compor os motivos da indenização, compreendendo que seria devido o valor de R$ 15.000,00 para esse fim. O que se demonstra, a exemplo das demais decisões, é que embora acertada a avaliação abusiva do assédio eleitoral e, portanto, passível de indenização, não se mostra razoável o valor das indenizações arbitradas, muito por não se reunir no arcabouço de fundamentos todos aqueles que revelem a ocorrência de múltiplas e gravíssimas lesões ao trabalhador e à sociedade.

Não é demais lembrar que a coação eleitoral, além de ferir direito de personalidade do trabalhador, sua autonomia e se configurar em crime, atenta contra o estado democrático de direito e, não sendo combatido a altura, viabiliza o retorno nefasto, ainda que sob outra roupagem, de um voto de cabresto, acompanhado de perseguição no ambiente de trabalho e, inclusive, na esfera privada do trabalhador, que passa a ter suas redes sociais monitoradas para avaliação de sua percepção política ou sua visão social de mundo[19]. Isso pode não apenas refletir nos contratos de trabalhos em curso, em razão das demissões arbitrárias, como pode impedir a

---

[18] BRASIL. 4ª Vara do Trabalho de Campina Grande/PB. *ATSum 0000794-95.2022.5.13.0023*, Juíza Maria Iris Diogenes Bezerra. Publicado em 11 jul. 2023. Disponível em: https://pje.trt13.jus.br/consultaprocessual/captcha/detalhe-processo/0000794-95.2022.5.13.0023/1. Acesso em 19 ago. 2023.

[19] SOARES, Marcelo Negri; LAGO, Andréa Carla de Moraes Pereira; JORGE, Welington Júnior. Liberdade de pensamento: assédio eleitoral e a proteção dos direitos da personalidade do trabalhador. In *Revista Direitos, Trabalho e Política Social,* Cuiabá, V. 9, n. 16, jan./jun. 2023. Disponível em: https://periodicoscientificos.ufmt.br/ojs/index.php/rdtps/article/view/15056/12401. Acesso em 25 ago. 2023, p. 120.

empregabilidade das pessoas, em evidente conduta discriminatória. No processo ora analisado, da 4ª Vara do Trabalho de Campina Grande/PB, registra-se que a Juíza determinou a remessa de cópia dos autos ao Ministério Público do Trabalho e Eleitoral em virtude dos fatos apurados.

Por fim, como último exemplo, traz-se a Ação Civil Pública n.º 0000275-57.2022.5.23.0051, da 1ª Vara do Trabalho de Tangará da Serra/MT, julgada pelo Juiz Mauro Roberto Vaz Curvo, em 15 maio 2023, cuja sentença, para o propósito deste trabalho, é a que mais se aproxima dos fundamentos e da finalidade reparatória que merece ser consagrada em casos de assédio eleitoral.

Em breve síntese, a empresa reclamada obrigava os seus funcionários a usar uma camiseta com dizeres alusivos à campanha de um dos candidatos à presidência, sendo a primeira camiseta com os dizeres "Deus, Pátria, Família e Liberdade", nas cores verde e amarela, tendo sido notificada pela Justiça Eleitoral, com recomendação expressa do Ministério Público do Trabalho para abster-se de tal conduta. Mesmo assim, manteve sua conduta, trocando referida camiseta por outra, com as mesmas cores, agora com os dizeres "Meu partido é o Brasil". É importante destacar que as campanhas políticas são uma modalidade de campanha publicitária e, como tal, valem-se das mesmas ferramentas de marketing, a exemplo de slogans, cores e músicas específicas, em associação a um determinado candidato, como se fosse um produto. Nesse sentido, a referência específica a uma dessas associações de marketing gera a identificação imediata do candidato, ainda que não se diga, expressamente, seu nome.

Na sua análise jurídica, o magistrado revelou um arcabouço de fundamentos que destacam as múltiplas lesões afetadas pela conduta abusiva da empresa. Citam-se:

> A Constituição Federal assegura como direito fundamental o pluralismo político (ar. 1, V), a liberdade de consciência, de convicção filosófica e política (arts. 1º, II e V; 5º, VI, VIII) e protege o exercício dos direitos de cidadania, o que indubitavelmente abrange o direito ao voto e a liberdade de escolher o candidato à Presidência da República que melhor atenda a seus interesses individuais ou sociais (arts. 14 CF c/c art. 60, §4º, II). Além da Constituição Federal, diversas

> normas internacionais consagram, como direito humano, a liberdade de consciência, de convicção filosófica e política e a vedam práticas discriminatórias por opinião política, como é o caso da Declaração Universal dos Direitos Humanos (arts. 1º, 2º, 7º, 12, 18 e 19), Pacto Internacional de Direitos Civis e Políticos (art. 25), Convenção Americana de Direitos Humanos – Pacto de San José da Costa Rica (art. 1º). Outrossim, o Código Eleitoral (artigos 299 e 301) criminaliza as condutas praticadas por empregadores, tomadores de serviços e terceiros, com o objetivo de interferir na escolha do voto. Ações como propagandas nos locais de trabalho são consideradas ilícitas pela legislação eleitoral (Lei 9.504/97 e Resolução TSE 23.610/2019), podendo inclusive caracterizar abuso de poder econômico [...]. Oportuno ressaltar, ainda, que o poder diretivo do empregador só pode ser exercido nos estritos limites e finalidades laborais, não podendo ele, empregador, invadir a esfera das liberdades e garantias fundamentais dos trabalhadores, sob pena de caracterização do abuso de direito, como também prática de ilícitos civis, criminais e trabalhistas, além da reparação por danos morais e materiais. Por todo exposto, concluo que a ré ao fornecer a camiseta praticou assédio eleitoral, além de ato discriminatório e abusivo, ante a intenção de interferir nos direitos ao livre exercício do voto e a manifestação política de seus empregados[20].

Em conclusão, considerando a gravidade da lesão e, ainda, considerando tratar-se de uma ação civil pública, cuja tutela apreciada referia-se à lesão a uma coletividade, o juiz condenou a empresa em danos morais coletivos no importe de R$ 150.000,00 (cento e cinquenta mil reais) e, ainda, condenou-a a cumprir obrigações de fazer e não fazer sob pena de multa no importe de R$ 50.000,00 por obrigação descumprida, acrescida de R$ 10.000,00, por trabalhador prejudicado.

Além disso, considerando os fatos apurados, o juiz também determinou expedição de ofícios para averiguação nas esferas competentes da Justiça Eleitoral, Ministério Público Federal e Ministério Público Estadual e seus correspondentes desdobramentos.

---

[20] BRASIL. 1ª Vara do Trabalho de Tangará da Serra/MT. *ACPCiv 0000275-57.2022.5.23.0051*. Juiz Mauro Roberto Vaz Curvo. Publicada em 15 maio 2023. Disponível em: https://pje.trt23.jus.br/consultaprocessual/detalhe-processo/0000275-57.2022.5.23.0051. Acesso em 19 ago. 2023.

Essa sentença certamente serve como paradigma para futuras análises de assédio eleitoral, quanto à sua fundamentação jurídica. Debruçando-se, contudo, sobre todos os seus fundamentos, embora sejam suficientes a sustentar a condenação, verifica-se, como em todas as demais sentenças e julgados analisados, haver omissão acerca dos fundamentos legais previstos na LGPD, conforme explicitados no item 1.4., quanto à violação da autodeterminação, aos dados pessoais sensíveis e, igualmente, sobre a forma de distribuição do ônus da prova. Cita-se a relevância dessa interpretação, que visa a proteção da parte hipossuficiente – premissa principiológica do Direito do Trabalho – na medida em que as eventuais ações julgadas improcedentes assim se deram pela insuficiência probatória, cujo ônus era atribuído ao trabalhador por força do art. 818, I, da CLT, ao invés de se valer do art. 42, § 1º, da LGPD para esse fim.

Nesse sentido, apesar de todas as violações contidas na conduta assediadora em análise, aparentemente, nas ações judiciais que dela trataram, quando provas haviam, os juízes e as juízas consideraram, em regra, um baixo potencial lesivo, o que se verifica pelo conjunto de fundamentos jurídicos usados e, por conseguinte, pelos baixos valores indenizatórios arbitrados a título de reparação civil, embora se trate de uma lesão de natureza gravíssima.

CONSIDERAÇÕES FINAIS

Com foco na liberdade de autodeterminação política, tomou-se como recorte histórico as violações cometidas no meio ambiente de trabalho em virtude das práticas de assédio eleitoral, em especial, nas eleições presidenciais, tanto de 2018 e, com mais ênfase, em 2022.

Como visto, essa conduta antijurídica afeta e contamina o meio ambiente do trabalho, assim como afeta direitos fundamentais e humanos do trabalhador vítima desse assédio, constrangendo-lhe, seja através de ameaças, seja através de benefícios extracontratuais, a submeter-se à orientação do candidato político elegível pelo empregador. Tal conduta gera uma plêiade de ofensas ao direito de personalidade do trabalhador, que pode, inclusive, desenvolver doenças psicossomáticas graves por essa razão. Demonstrou-se, ainda, que para além da

proteção constitucional fundamental e do trabalho e, ainda, aquela contida em normas internacionais sobre direitos humanos, também há tutela à proteção dos dados pessoais sensíveis, conforme previsto na LGPD que tutela, entre outras coisas, a autodeterminação e a convicção política das pessoas, em qualquer esfera.

Soma-se a isso a possibilidade de que a conduta praticada dentro do contrato de trabalho pode se configurar em crime eleitoral, atingindo-se coletivamente à sociedade, uma vez que a coação, valendo-se de qualquer subterfúgio, para que alguém vulnerável vote em determinado candidato, sem que haja respeito à sua convicção política, além de ser uma atitude criminosa, atenta contra o Estado Democrático de Direito.

Por fim, como propósito principal, a análise debruçou-se sobre os julgamentos advindos da Justiça do Trabalho e que apreciaram esse tema, tendo sido identificada uma diversidade na causas jurídicas determinantes para o reconhecimento do assédio e a responsabilização do agente assediador, mostrando-se, contudo, uma omissão da totalidade dos objetos jurídicos tutelados descritos no presente trabalho, o que, por certo, influencia a análise da gravidade da conduta e, por conseguinte, o arbitramento da quantia indenizatória devida às vítimas.

REFERÊNCIAS

ADORNO, Theodor W. *Educação e emancipação*. Tradução de Wolfgang Leo Maar. 3. ed. São Paulo: Paz e Terra, 2003.

BRASIL. Conselho Nacional de Justiça. *Protocolo para julgamento com perspectiva de gênero.* Grupo de Trabalho instituído pela Portaria CNJ n.º 27, de 2 de fevereiro de 2021. Disponível em https://www.cnj.jus.br/wp-content/uploads/2021/10/protocolo-18-10-2021-final.pdf. Acesso em 20 ago. 2023.

BRASIL. Ministério Público do Trabalho*. Assédio Eleitoral. Eleições 2022*: Relatório de atividades. Publicado em novembro de 2022.

BRASIL. Ministério Público do Trabalho em Mato Grosso. *Assédio eleitoral:* Justiça fixa multa após ameaça de demissão em massa em Rondonópolis. Publicado em 27 out. 2022. Disponível em https://www.prt23.mpt.mp.br/1882-assedio-eleitoral-justica-fixa-multa-apos-ameaca-de-demissao-em-massa-em-rondonopolis. Acesso em 20 jun. 2023.

BRASIL. Ministério Público do Trabalho em Mato Grosso. *MPT obtém liminar em face de empresária que confirmou prática de assédio eleitoral em reportagem*. Publicado em 27 out. 2022. Disponível em https://www.prt23.mpt.mp.br/1884-mpt-obtem-liminar-em-face-de-empresaria-que-confirmou-pratica-de-assedio-eleitoral-em-reportagem. Acesso em 20 jun. 2023.

BRASIL. Ministério Público do Trabalho em Mato Grosso. *MPT obtém liminar em face de supermercado de Nova Olímpia em ação para coibir assédio eleitoral*. Publicado em 27 out. 2022. Disponível em https://www.prt23.mpt.mp.br/1883-mpt-obtem-liminar-em-face-de-supermercado-de-nova-olimpia-em-acao-contra-assedio-eleitoral. Acesso em 20 jun. 2023.

BRASIL. Tribunal Regional do Trabalho da 4ª Região*. ROT 0020964-33.2019.5.04.0124.* Relator André Reverbel Fernandes. Publicado em 08 mar. 2023. Disponível em https://pesquisatextual.trt4.jus.br/pesquisas/rest/download/acordao/pje/uOSrE2htPJo6HyHeoSh0rQ. Acesso em 19 ago. 2023.

BRASIL, Tribunal Regional do Trabalho da 12ª Região, *ROT 0000190-47.2020.5.12.0019,* Relatora Ligia Maria Teixeira Gouvea, Publicado em 20 abr. 2022. Disponível em https://pje.trt12.jus.br/consultaprocessual/detalhe-processo/0000190-47.2020.5.12.0019. Acesso em 19 ago. 2023.

BRASIL. Tribunal Superior do Trabalho. Ag-AIRR-2451-06.2016.5.12.0025. Relator Min. Cláudio Brandão. Publicado em 27 abr. 2022. Disponível em https://jurisprudencia-backend2.tst.jus.br/rest/documentos/23df1e835b6c06b3b0e55e7eade3a32b. Acesso em 19 ago. 2023.

BRASIL. Tribunal Superior Eleitoral. *Partidos Políticos registrados no TSE*. Disponível em https://www.tse.jus.br/partidos/partidos-registrados-no-tse. Acesso em 16 ago. 2023.

BRASIL. Vara do Trabalho de Mafra/SC. *ATOrd 0001324-47.2022.5.12.0017*. Juíza Izabel Maria Amorim Lisboa. Publicado em 27 jul. 2023.

BRASIL. 1ª Vara do Trabalho de Tangará da Serra/MT. *ACPCiv 0000275-57.2022.5.23.0051*. Juiz Mauro Roberto Vaz Curvo. Publicada em 15 maio 2023. Disponível em https://pje.trt23.jus.br/consultaprocessual/detalhe-processo/0000275-57.2022.5.23.0051. Acesso em 19 ago. 2023.

BRASIL. 4ª Vara do Trabalho de Campina Grande/PB**.** *ATSum 0000794-95.2022.5.13.0023*, Juíza Maria Iris Diogenes Bezerra. Publicado em 11 jul. 2023. Disponível em https://pje.trt13.jus.br/consultaprocessual/captcha/detalhe-processo/0000794-95.2022.5.13.0023/1. Acesso em 19 ago. 2023.

CAMARA, Amanda Paoleli. Coronelismo nas eleições atuais: o protagonismo perigoso do assédio eleitoral no ambiente de trabalho. *In: Revista Economia e Globalização.* Publicado em 20 dez. 2022. Disponível em http://revistadedireito.catolicasc.org.br/index.php/revistadedireito/article/view/35. Acesso em 19 ago. 2023.

CARVALHO, Felipe Rodolfo de; PODOLAN, Plínio Gevezier. A reforma trabalhista e a ofensa ao direito humano de livre acesso à justiça: uma análise do duplo controle de verticalidade. In *Revista Magister de Direito do Trabalho.* N. 112, p. 51-76, Porto Alegre: Magister, 2023.

FELICIANO, Guilherme Guimarães; CONFORTI, Luciana Paula. Sobre o assédio eleitoral no Direito do Trabalho: as novas veredas do velho coronelismo à brasileira. In *Revista Direito UNIFACS – Debate Virtual,* n. 274, 2023. Disponível em https://revistas.unifacs.br/index.php/redu/article/view/8166/4805. Acesso em 25 ago. 2023.

MARANHÃO, Ney. Meio ambiente do trabalho: descrição jurídico-conceitual. In *Revista Direitos, Trabalho, e Política Social.* V. 2, n. 3, p. 80-117, Cuiabá, jul./dez. 2016.

MAZZUOLI, Valério de Oliveira; MARANHÃO, Ney; AZEVEDO NETO, Platon Teixeira de. Direitos Humanos e Direito Internacional Público: considerações à luz da tutela jurídico-internacional do ser humano que trabalha**.** *In: Revista de Direito do Trabalho e Seguridade Social*. V. 216, p. 239-272. São Paulo: Ed. RT, 2021.

SARLET, Gabrielle Bezzera Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) – L.13.709/2018. In *Revista de direitos fundamentais e democracia*, v. 26, n. 2, p. 81-106, mai./ago. 2021. Disponível em https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em 20 ago. 2023.

SOARES, Marcelo Negri; LAGO, Andréa Carla de Moraes Pereira; JORGE, Welington Júnior. Liberdade de pensamento: assédio eleitoral e a proteção dos direitos da personalidade do trabalhador. In *Revista Direitos, Trabalho e Política Social,* Cuiabá, V. 9, n. 16, jan./jun. 2023. Disponível em https://periodicoscientificos.ufmt.br/ojs/index.php/rdtps/article/view/15056/12401. Acesso em 25 ago. 2023.

9. TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO ANÁLISE DO CAPÍTULO IV, DA LGPD, SEGUNDO AS DIRETRIZES EMITIDAS PELA ANPD EM SEU GUIA ORIENTATIVO DE 2022

https://doi.org/10.36592/9786554600712-09

Rafael Louzada Nardin[1]

SUMÁRIO

1 Introdução; 2 Delimitação do conceito de "Poder Público" para fins de tratamento de dados pessoais; 3 Bases legais e princípios da LGFP mais pertinentes para o Poder Público; 4 Uso compartilhado de dados pessoais coletados pelo Poder Público – Análise do "Caso do IBGE"; 5 Considerações finais.

RESUMO

O presente texto tem como objetivo a formulação de estudo acadêmico sobre o regramento legal aplicado ao tratamento de dados pessoais promovido pelo poder público e como esse pode ser empreendido sem a lesão dos direitos de personalidade dos titulares dos dados tratados. Ao longo deste artigo, pretende-se priorizar o estudo das bases legais e princípios da Lei Geral de Proteção de Dados Pessoais (LGPD) mais pertinentes para Administração Pública, além de apresentar um estudo mais preciso sobre o compartilhamento de dados pessoais coletados por seus agentes. Nesse sentido, o texto foi construído de forma abordar os pontos mais relevantes sobre os artigos do Capítulo IV da LGPD em harmonia com as disposições orientativas emitidas pela Autoridade Nacional de Proteção de Dados do Brasil em sua guia publicado em 2022. A partir do arcabouço teórico trabalhado, entende-se como possível o tratamento de dados pessoais pelo poder público em prol do aumento da eficiência das prestações estatais sem a lesão do complexo jurídico da personalidade dos titulares dos dados tratados.
Palavras-chave: Tratamento de Dados Pessoais; Administração Pública.

---

[1] Advogado, bacharel em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). Pós-graduado em Direito Público pela Escola Superior da Magistratura Federal do Rio Grande do Sul (ESMAFE-RS). Pós-graduado em Direito Tributário pela Universidade Federal do Rio Grande do Sul (UFRGS). Mestrando em Direito pelo Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS).

1 INTRODUÇÃO

Com o desenvolvimento das tecnologias da informação, as últimas décadas foram marcadas pela mudança do perfil de riqueza. Mercados historicamente consolidados, como do petróleo e das telecomunicações, começaram a dar espaço para o crescimento de empresas que focaram sua atuação do desenvolvimento tecnológico. Companhias como a Google e a Meta se consolidaram como empresas multibilionárias que atuam com a chamada "commodity" do século 21: dados pessoais. O tratamento de dados pessoais (sejam eles vinculados à personalidade, ao consumo, etc) se mostra como uma das atividades que mais revolucionaram a economia mundial.

A correta compreensão de dados em grande escala proporciona mecanismo de análise de cenários e tendências extremamente fidedignos, resultando no alcance da tão almejada "eficiência", que seria a obtenção de máximo resultado com a utilização mínima de recurso. Frente a esses inúmeros benefícios proporcionados pelo tratamento de dados, naturalmente o Poder Público tem interesse nessa exploração, visto que vê na atividade uma ótima forma de promover o afinamento do instrumento de atuação estatal, especialmente em relação à promoção de políticas públicas. Tal interesse na tentativa de tornar a atuação administrativa mais assertiva é verdadeiro reflexo do princípio da eficiência consagrado no texto constitucional em seu Art. 37[2].

Entretanto, diferentemente do que ocorre no setor privado, em virtude de vários deveres legais e constitucionais que o poder público deve atender com sua atuação, como possibilitar o acesso à informação da atividade pública, o regramento a ser aplicado ao tratamento de dados dos órgãos e entidades públicas necessita uma atenção maior e diferenciada. Nessa perspectiva, o capítulo IV da Lei Geral de Proteção de Dados Pessoais (LGPD) prevê disposições legais específicas para

[2] Quanto ao princípio da eficiência administrativa, CELSO ANTÔNIO BANDEIRA DE MELLO alerta em sua doutrina que esse "é juridicamente tão fluido e de tão difícil controle ao lume do Direito, que mais parece um simples adorno agregado ao art. 37 ou o extravasamento de uma aspiração dos que buliram no texto. De toda sorte, o fato é que tal princípio não pode ser concebido (entre nós nunca é demais fazer ressalvas óbvias) senão na intimidade do princípio da legalidade, pois jamais uma suposta busca de eficiência justificaria". (MELLO, Celso Antônio Bandeira De. **Curso De Direito Administrativo.** 20 ed. rev. e atual. São Paulo: Malheiros, 2006. p. 109.)

regulamentar o uso de tratamento de dados pessoais pelo setor público, viabilizando assim o equilíbrio necessário para permitir que seja alcançado tanto a eficiência administrativa como a proteção do complexo jurídico da personalidade dos titulares dos dados tratados[3].

Esclarecida a atualidade e relevância do assunto, propõe-se com o presente estudo a construção de um breve panorama acerca do regramento aplicado ao tratamento de dados pessoais pelo poder público. Para tanto, pretende-se abordar os pontos mais pertinentes sobre os artigos do Capítulo IV da LGPD em harmonia com as disposições orientativas emitidas pela Autoridade Nacional de Proteção de Dados do Brasil em sua guia de 2022.

Proporcionando um ponto de vista científico sobre o tema, pretende-se também trazer alguns ensinamentos doutrinários e jurisprudenciais de maior pertinência sobre objeto de análise. Finalizando essas considerações introdutórias, importante destacar que a matéria possui extensão considerável, de forma que não poderia este texto se comprometer com uma análise integral e exaustiva de todos os pontos que a tangenciam. Dessa forma, propõe-se um breve aprofundamento das bases legais e dos princípios da LGPD que possuem maior pertinência ao setor público segundo a ANPD, como também o estudo do compartilhamento de dados pessoais coletados, especialmente o famoso "Caso do IBGE" julgado pelo Supremo Tribunal Federal.

2 DELIMITAÇÃO DO CONCEITO DE "PODER PÚBLICO" PARA FINS DE TRATAMENTO DE DADOS PESSOAIS

Preliminarmente, visto que o capítulo IV da LGPD prevê regramento específico para o tratamento de dados pessoais pelo Poder Público, necessário se faz

---

[3] "Deve-se se ter em mente que a maneira de como se dá o tratamento de dados pessoais pode afetar diretamente o direito à privacidade de qualquer indivíduo, por isso a importância de regulação da matéria, tendo em vista que todo cidadão tem o direito de ter acesso aos seus dados pessoais, o direito de retificá-los ou excluí-los, de decidir a respeito de seu destino e finalidade" (OLIVEIRA, A. C. S. de; DA SILVA ARAÚJO, D. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, *[S. l.]*, v. 16, n. 2, p. e5318, 2020. DOI: 10.18617/liinc.v16i2.5318. Disponível em: https://revista.ibict.br/liinc/article/view/5318. Acesso em: 30 ago. 2023. p. 3.)

esclarecer quais órgãos e entidades estão abarcados neste conceito. Analisando a primeira parte do caput do Art. 23 da lei brasileira de proteção de dados, conforme exposto no § único do Art. 1º da Lei de Acesso à Informação (Lei nº 12.527/11), será considerado como Poder Público: 1) a Administração Pública Direta, sendo eles os órgãos integrantes dos poderes executivo, legislativo, incluindo as cortes de contas, e judiciário e do Ministério Público; e 2) Administração Pública Indireta, sendo eles as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios[4].

Vale destacar que, quanto às empresas públicas e sociedades de economia mista, o legislador teve cuidado em estabelecer regramento específico, visto que, conforme regra geral prevista no caput do Art. 24 da LGPD, tais entidades deverão respeitar os mesmos regramentos dos agentes do setor privado, tendo em vista a necessidade de preservar o princípio constitucional da concorrência previsto no inciso IV do Art. 170 da Constituição Federal. Todavia, ciente da peculiaridade de algumas atuações desses personagens da Administração Pública Indireta, cuidou o legislador de estabelecer hipótese excepcional no parágrafo único do supramencionado artigo: observará o regramento específico do poder público de tratamento de dados pessoais todas as empresas públicas e sociedade de economia mista que estiverem operacionalizando políticas públicas (no âmbito da execução delas) e não atuarem em regime de concorrência.

Por fim, interessante ressaltar também que os §§ 4º e 5º do Art. 23 da LGPD, preveem a aplicação das disposições de tratamento de dados pelo setor público aos

---

[4] Quanto ao ponto, a ANPD em seu Guia Orientativo pontua que: "O art. 1º da LGPD é expresso quanto à aplicação da lei às pessoas jurídicas de direito público. O parágrafo único do mesmo artigo esclarece que as normas gerais contidas na LGPD "são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios". Já o art. 23, ao regulamentar o tratamento de dados pessoais pelo Poder Público, menciona as "pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação)". Este dispositivo, por sua vez, se refere aos "órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público". (BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 5. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.)

serviços notariais e de registro exercidos em caráter privado. Tal disposição se justifica pelo fato de tais agentes atuarem em face de delegação do poder público[5].

3 BASES LEGAIS E PRINCÍPIOS DA LGPD MAIS PERTINENTES PARA O PODER PÚBLICO

A partir da interpretação sistemática dos artigos do capítulo IV da LGPD, a Autoridade Nacional de Proteção de Dados (ANPD) asseverou em seu guia orientativo emitido em 2022 as bases legais e princípios previsto nos artigos 6º, 7º e 11 da lei brasileira de proteção de dados que possuem maior pertinência para a atuação estatal. Quanto às bases legais, a ANPD destacou quatro: 1) consentimento, previsto nos Art. 7º, I e Art. 11, I; 2) atendimento ao interesse público/legítimo, previsto no Art. 7º, IX; 3) cumprimento de obrigação legal ou regulatória, previsto nos Art. 7º, II e Art. 11, II, "a"; e 4) execução de políticas públicas, previsto nos Art. 7º, III e Art. 11, II, "b"[6].

Quanto ao consentimento, a própria lei define seu conceito no inciso XII do Art. 5º da LGPD como "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada"[7]. Em relação à essa base legal, a ANPD pontuou que tal autorização deve ser explicitamente intencional, devendo o titular dos dados ter total ciência dos fins de tratamento[8].

---

[5] "A regulação da LGPD aos serviços notariais e de registro está alinhada com a disciplina decorrente do art. 236, CF/1988, que estabelece um regime especial e sui generis a tais entidades, de caráter privado, mas por delegação do Poder Público. Nessa perspectiva, para tais entidades, é aplicada o mesmo regime da LGPD aplicável às pessoas jurídicas de direito público." (TAMER, Maurício. **LGPD**: comentada artigo por artigo: interpretação e aplicação da lei. 1. ed. São Paulo: Rideel, 2021. p. 213.)

[6] BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 6. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[7] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

[8] BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 6. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

Outra recomendação prevista no guia orientativo da ANPD é quando da não utilização dessa base legal. Em grande parte das oportunidades de tratamento de dados pelo poder público, o consentimento não se apresentará como a base legal mais apropriada, especialmente quando o tratamento for necessário para cumprimento de obrigações ou atribuições legais. Nesses casos, o exercício de prerrogativas estatais típicas transparece relação de desequilíbrio de forças entre os titulares dos dados e o poder público, não possuindo o cidadão efetivas condições de se manifestar livremente sobre tal tratamento[9].

A segunda base legal entendida como pertinente para o setor público pela ANPD é o atendimento de interesse legítimo. Diferentemente do consentimento, não existe definição legal objetiva e expressa no texto da LGPD sobre o "legítimo interesse", representando assim uma maior flexibilidade de aplicação, ou seja, passível de maior subjetividade de seu enquadramento e aplicação. Em virtude dessa condição, o próprio legislador tomou cuidado em relação à área de aplicação dessa base legal, tendo impossibilitado seu uso para tratamento de dados sensíveis, uma vez que não restou comtemplada no rol do Art. 11 da lei.

Destaca-se que tal condição peculiar, típica dessa base legal, é elemento reconhecido pela doutrina pátria. Conforme leciona em sua obra, Luis Carlos Buchain esclarece:

> Diferentemente dos demais fundamentos, o "legítimo interesse" não poderá ser avaliado isoladamente, pois – segundo a lei – deverá ser aplicado unicamente se não violar direitos e liberdades fundamentais do titular (Art. 10, II da LGPD), o que exige que esta política de tratamento de dados seja balanceada entre os interesses dos agentes de tratamento e aqueles do titular dos dados.[10]

Ainda sobre o "legítimo interesse", a Autoridade Nacional recomenda que seu uso seja evitado, de forma a priorizar-se as demais bases pelo poder público. Para

---

[9] BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 7. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[10] BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 45, p. 103-127, abr. 2021.

ANPD, tal base legal somente será indicada caso a utilização dos dados: 1) não seja compulsória ou; 2) a atuação estatal não seja baseada no exercício de prerrogativas estatais típicas que decorrem do cumprimento de obrigações e atribuições legais[11]. A sensibilidade dessa base legal é tamanha que pode ser constatada com facilidade no cotidiano contemporâneo exemplos de distorção maliciosa dessa base legal, como no caso do governo chinês que decidiu promover tratamento de dados pessoais com fim de catalogação do perfil político das pessoas e empresas sob a suposta justificativa de promoção da "segurança nacional"[12].

A terceira base legal destacada pela ANPD é o cumprimento de obrigação legal ou regulatória. Para a Autoridade, torna-se importante o esclarecimento dos dois tipos de atos normativos que serão aplicados no presente caso. O primeiro deles é a norma de conduta, sendo esse ato uma regra que disciplina um comportamento do poder público, ou seja, o tratamento de dados se mostra como parte central de regra específica sobre o ponto. De forma a exemplificar tal cabimento, é possível citar o caso do tratamento de dados pessoais dos servidores públicos empreendidos pelo próprio órgão público vinculado para fins de pagamento de salários e aposentadorias.

O segundo tipo de ato normativo pertinente para o presente estudo é a norma de organização. Tal modalidade de dispositivo se concretiza como normas que estruturam órgãos e entidades e estabelecem suas competências e atribuições. Assim, o emprego de tratamento de dados pessoais se forma como atividade correlata a obrigação principal do órgão público, a chamada prerrogativa estatal típica. Ilustrando a presente hipótese, pode-se referir o tratamento de dados pessoais empreendidos pelas Assembleias Legislativas em relação ao processo legislativo, visto que, naturalmente, documentos que circulam nesse processo como pareceres, atas de reunião e projetos de lei acabam por conter dados pessoais.

Por fim, a quarta e última base legal de maior pertinência para o setor público é a execução de políticas públicas. Para tanto, necessário se faz, além de se atentar

---

[11] BRASIL, op. cit., p. 8.

[12] VIDAL LIY, Macarena. China vai usar dados pessoais para catalogar cidadãos e empresas. **El País**, 2016. Disponível em: https://brasil.elpais.com/brasil/2016/10/20/internacional/1476970091_757096.html. Acesso em: 06 jun. 2023.

à abrangência já analisada neste texto da extensão do conceito de Administração Pública para fins de LGPD, tecer algumas considerações sobre aos contornos conceituais da expressão "política pública"[13]. A análise do texto legal resulta na conclusão de que tal definição não foi expressamente abordado pela lei brasileira de proteção de dados. Nesse ponto, a ANPD pontua no seu guia orientativo de que o setor público deve interpretar a "política pública" de forma ampla, "de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução"[14].

Vencidas as bases legais mais importantes para o tratamento de dados pessoais pelo Poder Público, interessante se apresenta o destaque de aspectos peculiares dos princípios da LGPD nesta seara[15]. O primeiro mandado de otimização a ser verificado é o princípio da finalidade, previsto no inciso I do Art. 6º da LGPD, que possui como definição legal: "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades"[16]. Segundo a ótica do setor

---

[13]Para CLARICE SEIXAS DUARTE, "a política pública deve visar à realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento dos resultados. A política pública, de acordo com essa concepção, está voltada à realização de direitos por meio de arranjos institucionais que se expressam em programas de ação governamental complexos. Trata-se de uma série de estratégias para fomentar o uso racional dos meios e recursos postos à disposição dos Poderes Públicos para desempenhar as tarefas próprias do Estado Social e Democrático de Direito." (DUARTE, Clarice Seixas. O ciclo das políticas públicas. In: SMANIO, Gianpaolo Poggio; BERTOLINI, Patrícia Tuma Martins (Orgs.). **O direito e as políticas públicas no Brasil**. São Paulo: Atlas, 2013. p. 18.)

[14]BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 12. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[15] "A Finalidade, a Adequação, a Necessidade, o Livre acesso, a Qualidade dos dados, a Transparência, a Segurança, a Prevenção e a Não Discriminação permeadas pelo princípio da boa-fé, perfazem a constelação principiológica da LGPD que, por óbvio, é emoldurada pelos princípios constitucionalmente previstos pela Carta de 1988 e se ampara em instrumentos jurídicos previstos em outras searas, para além do direito digital, como a civil, a penal e a consumerista. Assim, em uma análise mais pormenorizada dos dispositivos desse instrumento legal, podem ser apontados como desdobramentos do direito à proteção de dados, dentre outros, os direitos: ao livre acesso, à qualidade dos dados, à transparência, à segurança, à prevenção e à não discriminação." (RUARO, R. L.; SARLET, G. B. S. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) - L. 13.709/2018. **Revista direitos fundamentais & democracia (UniBrasil)**, v. 26, mai./ago., 2021. p. 85-86.)

[16]BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em:

público, a finalidade do tratamento de dados pessoais deve almejar uma finalidade pública, conceito esse que possui uma carga subjetiva muito relevante.

Assim, de forma a auxiliar os agentes públicos na identificação de tal conceito, a ANPD recomenda em seu guia que a finalidade pública será adequada caso:

> (i) legítima, isto é, lícita e compatível com o ordenamento jurídico, além de amparada em uma base legal, que autorize o tratamento; (ii) específica, de maneira que a partir da finalidade seja possível delimitar o escopo do tratamento e estabelecer as garantias necessárias para a proteção dos dados pessoais; (iii) explícita, isto é, expressa de uma maneira clara e precisa; e (iv) informada, isto é, disponibilizada em linguagem simples e de fácil compreensão e acesso ao titular dos dados[17].

Vale ressaltar também que a finalidade definida no tratamento originário de dados pessoais acaba por limitar diretamente o uso secundário/posterior dos dados pessoais colhidos em outras situações de tratamento. Ou seja, somente será possível o tratamento posterior de dados pessoais recolhidos a título de outra finalidade caso essa nova esteja em harmonia com a originária. Para averiguação de tal compatibilidade, a Autoridade Nacional recomenda a análise de 5 (cinco) panoramas:

> (i) o contexto e as circunstâncias relevantes do caso concreto; (ii) a existência de conexão fática ou jurídica entre a finalidade original e a que fundamenta o tratamento posterior; (iii) a natureza dos dados pessoais, adotando-se posição de maior cautela quando abrangidos dados sensíveis; (iv) as expectativas legítimas dos titulares e os possíveis impactos do tratamento posterior sobre seus direitos; e (v) o interesse público e a finalidade pública específica do

---

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

[17]BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 13. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

> tratamento posterior, bem como o seu vínculo com as competências legais dos órgãos ou entidades envolvidos[18].

Em sintonia com o princípio da finalidade, surgem outros mandados de otimização que acabam por ser verdadeiros desdobramentos desse. O primeiro seria o princípio da adequação, previsto no inciso II do Art. 6º, que "impõe a observância da compatibilidade entre o tratamento dos dados pessoais e as finalidades que são informadas ao titular, observado o contexto em que é realizado. Dessa forma, o tratamento do dado deve ser compatível com o propósito informado ao titular"[19].

Já o segundo desdobramento da finalidade é o princípio da necessidade, que direciona a atuação pública para coletar dados pessoais de forma a acessar apenas o mínimo necessário para atingimento da finalidade pública pretendida, ou seja, "abrangendo apenas os 'dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados' (art. 6º, III LGPD). É feita a avaliação se a finalidade que se almeja pode ser atingida por outros meios menos gravosos ao titular de dados"[20].

Finalizando o presente tópico, necessário se faz mencionar a pertinência dos princípios da transparência e do livre acesso no tratamento de dados pelo poder público. O princípio da transparência restou definido na LGPD como "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"[21]. Neste sentido, "impõe obrigações de cunho geral e que

---

[18]BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 15. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[19]BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

[20]BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 14. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[21]BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

demandam uma postura ativa do agente de tratamento, que tem o dever de disponibilizar as informações exigidas pela lei, independentemente de solicitação do titular"[22].

Já o princípio do livre acesso, definido legalmente como "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"[23], enfatiza a necessidade de o agente de tratamento disponibilizar mecanismos efetivos para que o titular possa solicitar e ter acesso facilitado e gratuito a determinadas informações referentes ao tratamento de seus dados pessoais[24].

4 USO COMPARTILHADO DE DADOS PESSOAIS COLETADOS PELO PODER PÚBLICO – ANÁLISE DO "CASO DO IBGE"

Outro ponto muito importante quando se fala de tratamento de dados pessoais pelo poder público, é a temática do uso compartilhado de dados colhidos por um órgão público por outros agentes do setor público e privado. Relembra-se que tal opção é de extrema importância para se alcançar a maior eficiência possível da atuação estatal administrativa, uma vez que essa poderia basear-se em parâmetros mais fidedignos com a realidade.

---

[22]BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 14. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

[23]BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

[24]Quanto ao dever geral de transparência, MAURÍCIO TAMER destaca que "a LGPD busca trazer transparência à Administração Pública para com o titular de dados pessoais, não só por conta do previsto no seu conjunto principiológico, mas também pela sua própria lógica de regulação. O que faz o inc. I, nessa perspectiva, é acrescentar outros detalhes de como a transparência deve ser aplicada às pessoas de direito público interno. (...) Nesse sentido, cumpre mencionar que a Lei de Acesso à Informação traz disciplina específica sobre quais informações mínimas que devem ser disponibilizadas sobre os seus serviços no seu art. 8°. Por conta do diálogo entre a LGPD e a LAI, esses requisitos devem ser também aplicados em relação às informações sobre o tratamento de dados pessoais." (TAMER, Maurício. **LGPD**: comentada artigo por artigo: interpretação e aplicação da lei. 1. ed. São Paulo: Rideel, 2021. p. 210.)

Tendo a LGPD definido no inciso XVI do Art. 5º “uso compartilhado”[25], o compartilhamento de dados pelo poder público é temática regulada com cuidado pelo legislador nos Arts. 25, 26 e 27. Preliminarmente, previu-se a necessidade de manejo dos dados pessoais tendo em vista a praticabilidade do exercício do compartilhamento, pois se estabeleceu que esses devem ser formatados de maneira interoperável e estruturada[26]. Além disso, o Art. 26 da LGPD destaca que tal compartilhamento somente poderá ser realizado para atendimento de duas finalidades específicas: execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas.

O parágrafo 1º do Art. 26, da LGPD inaugura a discussão sobre a possibilidade ou não de compartilhamento de dados pessoais colhidos pelo poder público com entidades privadas. Inicialmente, é estabelecido uma regra geral na qual é vedado tal compartilhamento, tendo-se especificado nos incisos do § 1º de referido artigo as hipóteses excepcionais. Ou seja, será possível o compartilhamento de dados pessoais pelo poder público com entidade privada quando: 1) estiver se tratando de caso de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado; 2) casos em que os dados forem acessíveis publicamente; 3) quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres; ou 4) na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de

---

[25]“Art. 5º Para os fins desta Lei, considera-se: (...) XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;” (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.)

[26]MAURÍCIO TAMER esclarece que: “O formato interoperável é aquele que revela a capacidade de sistemas trabalharem em conjunto ou de operarem em conjunto de modo a viabilizar a troca e a gestão conjunta, compartilhada e mais eficiente. A preocupação do dispositivo é evitar a existência de sistemas que não dialogam entre si e que, por isso, venham a prejudicar o desenvolvimento das tarefas. Preza pela eficiência de sistemas e procedimentos e estruturas incomunicáveis". (TAMER, Maurício. op. cit. p. 214-215.)

fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades[27].

Por fim, o Art. 27 da LGPD estabelece a obrigação de informação à Autoridade Nacional da comunicação ou do uso compartilhado de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado. Essa obrigação apenas é dispensada em caso de se tratar de: 1) hipótese de dispensa de consentimento; 2) nos casos de uso compartilhado em que a publicidade se dá conforme dispõe inciso I do art. 23; e 3) demais hipóteses excepcionais comentadas do parágrafo 1º do Art. 26 da LGPD.

Tendo em vista a relevância que o uso compartilhado de dados tem para o aprimoramento da atuação estatal, e visando que tal uso seja feito de forma a respeitar as diretrizes da LGPD, a Autoridade Nacional estabeleceu no seu guia orientativo alguns elementos que são entendidos como essenciais para o devido uso compartilhado de dados, são eles: formalização e registro, objetivo e finalidade, a duração do tratamento, a prevenção e segurança, entre outros elementos importantes.

Quanto à formalização e registro do compartilhamento, a ANPD recomenda que seja instaurado processo administrativo, no qual constarão os documentos e as informações pertinentes, incluindo análise técnica e jurídica, conforme o caso, que exponham a motivação para a realização do compartilhamento e a sua aderência à legislação em vigor. Além disso, é indicado que o compartilhamento seja firmado em ato formal, seja como contrato, convênio ou instrumento congênere firmado entre as partes[28].

---

[27]Quanto ao caráter de excepcionalidade do compartilhamento de dados pessoais coletados pelo poder público com o setor privado, TAMER relembra a necessidade de observância do princípio da necessidade: "Explicando o caput e reforçando a preocupação quanto aos riscos do compartilhamento de dados pessoais entre os entes públicos e os entes privados, o § 1° define que a administração pública não pode transferir dados pessoais a entes privados como regra. A transferência, inclusive, que é uma das operações contempladas no conceito de uso compartilhado. (...) É importante ter em vista, ainda, que a transferência deve observar a estrita finalidade do compartilhamento e, também, contemplar apenas os dados estritamente necessários para tanto." (TAMER, Maurício. **LGPD**: comentada artigo por artigo: interpretação e aplicação da lei. 1. ed. São Paulo: Rideel, 2021. p. 216.)

[28] BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 17. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

Quanto ao objetivo e finalidade do compartilhamento, ressalta-se que os dados pessoais, objeto de compartilhamento, devem ser indicados, em conformidade com o princípio da necessidade, de forma objetiva e detalhada, limitando-se ao que for estritamente necessário para as finalidades do tratamento. A finalidade deve ser específica, vinculando precisamente a qual iniciativa, ação ou programa será executado ou, ainda, de qual atribuição legal será cumprida mediante o compartilhamento dos dados pessoais.

Em relação à determinação de duração finita do tratamento, tal previsão se mostra extremamente relevante, visto que proporciona a reavaliação periódica do instrumento que autorizou o compartilhamento, possibilitando sua adequação a novas disposições legais e regulamentares ou a previsão de novas medidas de segurança, de acordo com as tecnologias disponíveis. Em consonância com os princípios da transparência e do livre acesso, deve-se assegurar a disponibilização de informações claras, precisas e facilmente acessíveis aos titulares sobre a realização do compartilhamento e sobre como exercer seus direitos.

Ponto de extrema relevância para perfeito desfecho do compartilhamento é o estabelecimento de medidas de segurança, técnicas e administrativas, que serão adotadas para proteção em face de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais coletados. Quanto à extensão e profundidade dessas medidas, devem essas ser proporcionais aos riscos às liberdades civis e aos direitos fundamentais dos cidadãos envolvidos no caso concreto[29].

Destaca-se que existem inúmeros outros elementos que devem compor o instrumento de compartilhamento de dados como a definição do ônus financeiro, da possibilidade ou não de uso secundário desses dados, etc, todavia, a presente oportunidade não permite se alongar em demasia no ponto. Finalizando o presente tópico, de forma a ilustrar o presente estudo, pertinente se mostra a apresentação de breves considerações sobre o julgamento em conjunto das ações diretas de

---

[29] BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. p. 19. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

inconstitucionalidade nº 6387, nº 6388, nº 6389, nº 6390 e nº 6393, conhecidas pela comunidade jurídica como "Caso do IBGE"[30].

Assim, em um cenário de pandemia, foi promulgado a Medida Provisória nº 954/2020[31] que determinava o compartilhamento de dados pessoais de mais de 200 milhões de brasileiros que estavam contidos nas empresas de telefonia com o Instituto Brasileiro de Geografia e Estatística - IBGE. A justificativa veiculada à época era que tais dados seriam utilizados para municiar os gestores da saúde pública a desenvolverem estratégias mais efetivas de combate a pandemia, visto que não estava sendo possível a realização de entrevistas em caráter presencial de pesquisas domiciliares.

Muitas entidades civis entenderam que tal compartilhamento se mostrava totalmente desproporcional, de forma a ferir inúmeros direitos fundamentais dos brasileiros. Assim foram ajuizadas 5 (cinco) ações diretas de inconstitucionalidade de forma a questionar o STF sobre a constitucionalidade ou não dessa MP. Sobreveio decisão do Supremo no sentido de reconhecer a inconstitucionalidade da medida executiva, pontuando, em síntese: ausência de demonstração de interesse público legítimo para justificar o compartilhamento; não foi estabelecido medidas de segurança, sejam elas técnicas ou administrativas, para previr o acesso não autorizado ou ilícito de tal informação e o combate a pandemia não poderia justificar o atropelo de direitos fundamentais dos brasileiros[32].

---

[30] BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387**. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA: DEFERIMENTO. [...]. Requerente: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Requerido: Presidente da República. Relator(a): Rosa Weber, 07/05/2020, Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 26 de junho de 2023.

[31] BRASIL. **Medida provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em 19 de junho de 2023.

[32] Acerca do compartilhamento de dados públicos, Douglas Araújo e Adriana Carla de Oliveira destacam que: "surge um grande desafio aos gestores públicos que é o de conciliar a transparência que deve reger os atos da administração pública e, ao mesmo tempo, observar o regime jurídico de

CONSIDERAÇÕES FINAIS

O aprimoramento da assertividade e agilidade das ferramentas tecnológicas de tratamento de dados não deve ser analisado como fenômeno negativo para o desenvolvimento da humanidade. Pelo contrário, deve-se reconhecer que tais inovações digitais estão à disposição das pessoas para se tornarem mais produtivas e eficientes em seus ofícios e atribuições. Frente à notável incremento de produtividade alcançado pelo uso de tratamento de dados, naturalmente o Poder Público possui interesse na sua exploração, sendo esse fenômeno fato não só possível, mas também imperioso. Deve-se lembrar que a máquina pública nada mais é do que uma representação coletiva dos interesses de todos os cidadãos que a compõe, de forma que o melhoramento de sua eficiência é interesse óbvio e almejado por todos, visto que proporcionará cada mais uma melhor aplicação dos recursos colhidos da sociedade brasileira.

Entretanto, conforme podemos analisar nos exemplos contemporâneos citados ao longo do texto, quando se explora tratamento de informações que possuem uma sensibilidade extrema, torna-se evidente que o seu manuseio demanda a observância de regramentos rígidos que estão previstos prioritariamente para proteção do complexo jurídico de personalidade dos titulares dos dados pessoais tratados. É importante pontuar que se entende possível o atingimento de um equilíbrio saudável na presente matéria, apresentando-se como possível a utilização pelo poder público do tratamento de dados pessoais para aprimoramento do instrumento estatal de promoção de políticas públicas sem a ofensa dos direitos inerentes aos titulares dos dados.

Relembra-se que esse equilíbrio é muito estreito, de forma que tal desvirtuamento poderá deslocar o cenário brasileiro de legitimidade para

---

proteção de dados inaugurado pela LGPD. Muito embora possa se enxergar uma dicotomia entre esses temas, um alinhamento entre a Autoridade Nacional de Proteção de Dados (ANPD) e os órgãos de controle, a exemplo da Controladoria-Geral da União, será crucial para conciliação do direito à proteção de dados com a transparência pública, a partir da elaboração de normas que detalhem o regramento, limites e alcance da LGPD, sobretudo no campo dos dados públicos, dados abertos e governamentais." (OLIVEIRA, A. C. S. de; DA SILVA ARAÚJO, D. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, [S. l.], v. 16, n. 2, p. e5318, 2020. DOI: 10.18617/liinc.v16i2.5318. Disponível em: https://revista.ibict.br/liinc/article/view/5318. Acesso em: 30 ago. 2023. p. 3)

abusividade, assemelhando-se ao panorama tratado na famosa obra literária "1984" do autor britânico George Orwell. Assim, entende-se que a revisitação da presente matéria pela academia se mostra como fenômeno muito benefício para desenvolvimento e atualização científica do regramento aplicado ao tratamento de dados pelo poder público, proporcionando conclusões mais maduras e contemporâneas que serão base e fundamentos das futuras manifestações do Poder Judiciário brasileiro.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. **Tratamento de Dados Pessoais pelo Poder Público**. Versão 1.0. Brasília: ANPD, Jan 2022. Guia Orientativo. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em 19 de junho de 2023.

BRASIL. **Medida provisória nº 954, de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em 19 de junho de 2023.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6387**. MEDIDA CAUTELAR EM AÇÃO DIRETA DE INCONSTITUCIONALIDADE. REFERENDO. MEDIDA PROVISÓRIA Nº 954/2020. EMERGÊNCIA DE SAÚDE PÚBLICA DE IMPORTÂNCIA INTERNACIONAL DECORRENTE DO NOVO CORONAVÍRUS (COVID-19). COMPARTILHAMENTO DE DADOS DOS USUÁRIOS DO SERVIÇO TELEFÔNICO FIXO COMUTADO E DO SERVIÇO MÓVEL PESSOAL, PELAS EMPRESAS PRESTADORAS, COM O INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. FUMUS BONI JURIS. PERICULUM IN MORA. DEFERIMENTO. [...]. Requerente: Conselho Federal da Ordem dos Advogados do Brasil - CFOAB. Requerido: Presidente da República. Relator(a): Rosa Weber, 07/05/2020, Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 26 de junho de 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/lei/l14020.htm. Acesso em 19 de junho de 2023.

BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 45, p. 103-127, abr. 2021.

DUARTE, Clarice Seixas. O ciclo das políticas públicas. In: SMANIO, Gianpaolo Poggio; BERTOLINI, Patrícia Tuma Martins (Orgs.). **O direito e as políticas públicas no Brasil**. São Paulo: Atlas, 2013.
MELLO, Celso Antônio Bandeira De. **Curso De Direito Administrativo**. 20 ed. rev. e atual. São Paulo: Malheiros, 2006.

OLIVEIRA, A. C. S. de; DA SILVA ARAÚJO, D. O compartilhamento de dados pessoais dos beneficiários do auxílio emergencial à luz da Lei Geral de Proteção de Dados. **Liinc em Revista**, *[S. l.]*, v. 16, n. 2, p. e5318, 2020. DOI: 10.18617/liinc.v16i2.5318. Disponível em: https://revista.ibict.br/liinc/article/view/5318. Acesso em: 30 ago. 2023.

RUARO, R. L.; SARLET, G. B. S. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) - L. 13.709/2018. **Revista direitos fundamentais & democracia (UniBrasil**), v. 26, p. 81-106, mai./ago., 2021.

TAMER, Maurício. **LGPD**: comentada artigo por artigo: interpretação e aplicação da lei. 1. ed. São Paulo: Rideel, 2021.

VIDAL LIY, Macarena. China vai usar dados pessoais para catalogar cidadãos e empresas. **El País**, 2016. Disponível em: https://brasil.elpais.com/brasil/2016/10/20/internacional/1476970091_757096.html. Acesso em: 06 jun. 2023.

10. INTERNET DAS COISAS, CIDADES INTELIGENTES E O DIREITO À PRIVACIDADE DO CIDADÃO

 https://doi.org/10.36592/9786554600712-10

Taina Daniele Werle[1]

SUMÁRIO

1. Introdução; 2. A Evolução da Internet; 3. Internet das Coisas e Cidades Inteligentes; 3.1. Origem e Evolução da Internet das Coisas; 3.2. Conceito(s) de IOT e Exemplos de Uso Atual; 3.3. IOT e Cidades Inteligentes; 4. Privacidade X IOT e Cidades Inteligentes; 4.1. A Questão da Privacidade na Era Digital. 4.2. Problemática da Proteção da Privacidade X IOT e Cidades Inteligentes; 5. Considerações Finais. Referências.

1 INTRODUÇÃO

Em seus primeiros 40 anos de uso, a internet foi marcada, principalmente, por conectar pessoas, seja por trocas de e-mails, fóruns, sites ou redes sociais que coletam e distribuem dados. Atualmente, tem sido utilizada também para promover a conexão de dispositivos, máquinas e outros objetos, por redes com ou sem fio, modo a criar a chamada Internet das Coisas (IoT)[2].

Essa evolução foi permitida pelo crescente incremento das infraestruturas de redes e pela popularização da internet, que tornaram esta uma plataforma global e que proporciona que objetos inteligentes se comuniquem de forma autônoma[3]. Há dificuldade, todavia, de uma conceituação mais restrita de IoT. A ideia de uma rede mundial de objetos conectados e que possam trocar informações entre si é ampla, o

---

[1] Advogada. Mestranda em Direito pela PUCRS, na Área de Concentração de Fundamentos Constitucionais do Direito Público e do Direito Privado e na Linha de Pesquisa de Direito, Ciência, Tecnologia & Inovação. Bolsista CAPES. Especialista em Direito Tributário pela FGV. E-mail: werle.taina@edu.pucrs.br. Currículo Lattes: http://lattes.cnpq.br/956764875528022.
O presente trabalho foi realizado com apoio da PUCRS através do PROEX – CAPES.

[2] SANTOS, Carlos Cesar; SALES, Jefferson De Araujo. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.

[3] Ibid.

que possibilita que várias tecnologias diferentes acabem sendo explicadas através do nome “Internet das Coisas”[4].

Também relacionado ao desenvolvimento da internet e da IoT surge a ideia de implementação de tecnologia para gestão das cidades, em conjunto com a adoção de novos mecanismos para aprimorar a eficiência administrativa e os serviços prestados pelo poder público, proporcionando a criação de “Cidades Inteligentes”.

Concomitantemente às vantagens que a tecnologia de objetos interconectados pode oferecer, surgem também questionamentos sobre os riscos dessa interconexão, na esfera pública e na esfera privada, para a proteção da privacidade dos cidadãos.

Nesse contexto, o presente estudo busca avaliar o uso da Internet das Coisas e o desenvolvimento de Cidades Inteligentes com vistas a eventuais impactos na esfera de proteção da privacidade dos cidadãos.

Para tanto, será abordada, inicialmente, a evolução da internet até permitir a criação da “Internet das Coisas”, em continuidade, abordaremos a Internet das Coisas, sua origem e usos, bem como as Cidades Inteligentes; por fim, será tratado o direito à privacidade em linha com o uso de IoT e o desenvolvimento de Cidades Inteligentes.

2 A EVOLUÇÃO DA INTERNET

O conceito de Internet das Coisas está alinhado com a evolução da internet, mais especificamente com a denominada Web 3.0[5]. Assim sendo, antes de adentrar especificamente no conceito de Internet das Coisas, cabe realizar uma breve explicação sobre o surgimento da internet e a sua evolução até alcançar o patamar atual.

---

[4] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.

[5] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023

Conforme definição constante do art. 5º do Marco Civil da Internet, a internet pode ser entendida como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes", sendo considerado como terminal qualquer dispositivo ou computador que se conecte à internet[6].

A internet começou a fazer parte efetivamente da vida social brasileira em 1994, tornando-se um ambiente de relacionamento virtual que, até hoje, é amplamente utilizado para as mais diversas finalidades. Em 1994, os recursos da rede mundial, até então restritos ao meio acadêmico e algumas comunidades, foram disponibilizados ao público brasileiro de forma ampla, entretanto, a rede em si, surgiu bem antes, ao final da década de 1960[7].

A história do surgimento da internet remonta aos tempos da Guerra Fria, quando emergiram os conceitos de conectividade. Estimulado pelo desenvolvimento de tecnologias pela União Soviética, que havia lançado em órbita seu primeiro satélite espacial artificial, o Sputnik, em 1957, o Departamento Nacional de Defesa Norte-Americano ganhou um novo integrante, a *Advanced Research Projects Agency* (ARPA – Agência de Pesquisa e Projetos Avançados), criada com o objetivo de desenvolver pesquisas de informação para o serviço militar[8].

Como resultado desse esforço do sistema de defesa dos Estados Unidos para dotar a comunidade acadêmica e militar de uma rede de comunicações[9] que fosse além de um sistema de comunicação, também um sistema de defesa, que

[6] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 abr. 2023.
[7] LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013. Disponível em: http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em: 08 abr. 2023.
[8] ROCHA, G. C da; SOUZA FILHO, V. B de. Da guerra às emoções: história da internet e o controverso surgimento do Facebook. **Encontro Regional Norte de História da Mídia**, v. 4, 2016. Disponível em: http://www.alcarnorte.com.br/wp-content/uploads/alcar2016_da_guerra_as_emocoes_historia_da_internet_e_o_controverso_surgimento_do_facebook.pdf. Acesso em: 08 abr. 2023.
[9] LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013. Disponível em: http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em: 08 abr. 2023.

informasse sobre ataques terroristas e pudesse sobreviver a um ataque nuclear, surge o projeto ARPANET[10 11].

Em sua origem, a ARPANET era um projeto bélico, que garantiu a possibilidade de realizar transferência de voz e imagem através de uma rede interconectada[12]. O projeto ARPANET foi o embrião da rede mundial de computadores, da internet que conhecemos atualmente[13]. A intenção do projeto era alcançar uma comunicação sem falhas por meio de uma rede de computadores que utilizaria o protocolo TCP/IP para se comunicar[14].

Ao contrário das outras redes existentes, esta rede deveria permitir que cada equipamento fosse relativamente autônomo e que a comunicação ocorresse de forma distribuída, ou seja, de modo que, ainda que parte da rede fosse afetada, o restante – que não foi objeto de agressão – poderia manter-se em operação[15].

No começo da década de 1980, com a consolidação do protocolo TCP/IP como um meio de comunicação entre vários computadores, passou-se à comercialização das primeiras máquinas com acesso (Arpanet 8800, Apple I e II), favorecendo-se a exponenciação e a difusão do uso da internet como um ambiente digital. Nos anos que se seguiram, verificou-se a criação de LANs, PCs e workstations e, com isso, a internet foi ficando mais popular.[16]

Até o final de 1980, apesar de observar-se já uma expansão da conexão entre computadores e uma maior acessibilidade, principalmente no que se refere a máquinas instaladas em laboratórios de pesquisa, a internet não possuía, ainda, o amplo acesso e a "cara amigável" que conhecemos hoje[17].

---

[10] ROCHA, G. C da; SOUZA FILHO, V. B de. op. cit.
[11] LINS, Bernardo Felipe Estellita. op. cit.
[12] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.
[13] LINS, Bernardo Felipe Estellita. op. cit.
[14] MAGRANI, Eduardo. op. cit.
[15] LINS, Bernardo Felipe Estellita. op. cit.
[16] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.
[17] ROCHA, G. C da; SOUZA FILHO, V. B de. Da guerra às emoções: história da internet e o controverso surgimento do Facebook. **Encontro Regional Norte de História da Mídia**, v. 4, 2016. Disponível em: http://www.alcarnorte.com.br/wp-content/uploads/alcar2016_da_guerra_as_emocoes_historia_da_internet_e_o_controverso_surgimento_do_facebook.pdf. Acesso em: 08 abr. 2023.

No final da década de 1980, com a internet já estabilizada como uma comunidade, ocorreu mais um avanço através do *Conseil Européen pour la Recherche Nucléaire* (CERN), que foi a criação do que conhecemos hoje como WWW ou Web, o principal acesso à internet no mundo. Necessário destacar que, embora o termo Web tenha sido utilizado como sinônimo de internet, não se confunde com esta. Como destaca Magrani, "Web é um termo simplificado de World Wide Web, que consiste em apenas uma das várias ferramentas de acesso à internet. A Web usa a internet, mas ela em si não é a internet" [18].

A Web, portanto, seria uma aplicação que permite o compartilhamento de arquivos e que possui o *browser* – navegadores como o Chrome – como ferramenta de acesso. Usualmente, é através da Web que acessamos a internet[19].

A partir da apresentação do WWW por Tim Bernes Lee, em 1989, os avanços da internet se exponenciaram[20]. A Web foi se propagando com e pela internet e sua rápida adoção exigiu a adaptação tecnológica para novos contextos de uso[21]. Sua popularização acabou dando início à revolução digital[22], de tal modo que hoje é possível falar sobre a internet em gerações, como Web 1.0, 2.0, 3.0 e até 4.0 (alguns mencionam 5.0).

A Web 1.0 é aquela que surgiu na década de 1980, caracterizando-se pela possibilidade de conexão entre pessoas, porém sem permitir grande interação entre usuário e sites, uma vez que estes eram "somente leitura"[23]. Ademais, a produção dos conteúdos mostrava-se restrita a alguns usuários com conhecimento técnico elevado e a quantidade de conteúdos produzidos era considerada baixa, tendo em vista a demanda[24].

---

[18] MAGRANI, Eduardo. op. cit.

[19] Ibid.

[20] ROCHA, G. C da; SOUZA FILHO, V. B de. op. cit.

[21] DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, 2018. Disponível em: http://cm-kls-content.s3.amazonaws.com/LIVROS_UNOPAR_AEDU/Tend%C3%AAncias%20Do%20Marketing%20Digital.pdf. Acesso em: 08 abr. 2023.

[22] MAGRANI, Eduardo. op. cit.

[23] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.

[24] DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, 2018. Disponível em:

A ausência de comunicação e de interação é característica da Web 1.0, que ficou conhecida como a "Web do Conhecimento" pelo seu impacto através da disponibilização elevada de informações, das mais variadas, em diversas páginas[25].

A Web 2.0, por sua vez, definida em 2004, pode ser vista como a "Web da Comunicação" ou "Web da Sabedoria"[26] em razão da grande interatividade que viabilizou[27]. Através dela houve a ruptura do modelo linear até então utilizado, passando a ser observada uma via de mão dupla, onde o consumidor de conteúdo passava a ser também produtor, possibilitando, dessa forma, o aumento de informações disponíveis[28] [29].

Nessa fase, a Web adquire um caráter mais colaborativo e de interação constante com a expansão de plataformas como redes sociais, blogs, dentre outros[30]. Entre os anos 2000 e 2009, por exemplo, os endereços eletrônicos, já se apresentam de forma mais interativa na busca pela participação dos usuários[31].

A Web 3.0, por sua vez, diversamente da Web 2.0 que permitia somente a interação de pessoas, utiliza-se da internet para promover o cruzamento de dados. Enquanto a Web 2.0 foca na criatividade e na produção de conteúdo, a Web 3.0 foca nos dados e na interconexão de objetos. Embora o conceito de Web 3.0 não seja bem definido, é possível distingui-lo dos demais em razão dos novos polos de conexão que são verificados, já que a conexão e interação deixa de ser somente entre pessoas e passa a ser também entre objetos e pessoas e entre objetos e outros objetos, relacionando-se com a ideia de Internet das Coisas[32].

---

http://cmcontent.s3.amazonaws.com/LIVROS_UNOPAR_AEDU/Tend%C3%AAncias%20Do%20Marketing%20Digital.pdf. Acesso em: 08 abr. 2023.

[25] DECARLI, Gian Carlo. op. cit.

[26] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. A Web 4.0 e os Riscos à Democracia. **Revista Em Tempo,** [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3132>. Acesso em: 08 abr. 2023.

[27] DECARLI, Gian Carlo. op. cit.

[28] Ibid.

[29] MAGRANI, Eduardo. op. cit.

[30] Ibid.

[31] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. op. cit.

[32] MAGRANI, Eduardo. op. cit.

A Web 3.0 teria surgido em 2006, entretanto, seu reconhecimento se estendeu entre 2010 e 2019[33]. Também é denominada de "Web Semântica" ou "Web Inteligente" e possui como objetivo possibilitar a extração de conteúdo da Web para auxiliar o computador a processar, compreender e responder consultas, permitindo que pessoas e computadores trabalhem em cooperação. Em outras palavras, "busca por meio de suas tecnologias estabelecer padrões para publicação, armazenamento e recuperação de informações na Web"[34].

Essa nova geração permitiu a vinculação, integração e análise de dados com o objetivo de obter novos fluxos de informação, passando o computador a personalizar e otimizar pesquisas, bem assim direcionar anúncios conforme o comportamento e preferências dos seus usuários[35].

Além da definição de Internet das Coisas, relacionada com a Web 3.0, já vem ocorrendo uma disseminação de um conceito de Internet de Tudo (*Internet of Everything,* IoE). A princípio, não existem diferenciações claras e substanciais entre IoT e IoE, mas há quem defenda que a IoT seria um estágio na busca da IoE[36].

Ainda no que tange à evolução da internet, cabe salientar que já existem definições e previsões para as próximas Webs, dada a evolução cada vez mais veloz, quais sejam, Web 4.0 e 5.0.

A Web 4.0 teria seu marco temporal em 2020, entretanto, ainda não há uma definição clara e uníssona sobre a sua caracterização. Estabelece-se que esta geração avançaria no uso da inteligência artificial e da big data, permitindo o aumento do uso e interpretação de grande volume de dados, de forma automática[37].

Há quem reconheça já a Web 5.0, também chamada de "Web Sensorial-Emotiva", cujo objetivo seria desenvolver computadores que possam interagir com

---

[33] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. A Web 4.0 e os Riscos à Democracia. **Revista Em Tempo,** [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3132>. Acesso em: 08 abr. 2023.
[34] DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, 2018. Disponível em: http://cm-kls-content.s3.amazonaws.com/LIVROS_UNOPAR_AEDU/Tend%C3%AAncias%20Do%20Marketing%20Digital.pdf. Acesso em: 08 abr. 2023.
[35] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. op. cit.
[36] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.
[37] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. op. cit.

humanos e tornem-se itens essenciais no dia a dia, estando em progresso já, segundo Schroeder e Silva, a criação de equipamentos eletrônicos capazes de julgar emoções e expressões faciais humanas[38]. Fala-se também em "Web Simbiótica", que integraria de forma gradual a tecnologia ao ser humano, envolvendo sentimentos e emoções, modo a criar um "cérebro paralelo".[39]

Tais definições ainda são um tanto quanto vagas, principalmente se considerarmos que o conceito de Web 3.0 e Web 4.0 ainda não estão completamente consolidados, bem assim, a própria denominação de Web 2.0 fora alvo de críticas, de qualquer sorte, há grande possibilidade de, no futuro (talvez não tão distante) verificarmos o uso maior de inteligência artificial para a criação de uma tecnologia mais potente e eficiente[40].

Realizada a apresentação breve da evolução da internet, passamos ao estudo mais detalhado da Internet das Coisas e das Cidades Inteligentes.

3 INTERNET DAS COISAS E CIDADES INTELIGENTES

3.1 ORIGEM E EVOLUÇÃO DA INTERNET DAS COISAS

A ideia de uma rede mundial de objetos conectados e que possam trocar informações entre si é ampla, consequentemente, várias tecnologias diferentes podem acabar sendo explicadas através do nome "Internet das Coisas"[41].

A origem da Internet das Coisas está ligada à tecnologia RFID – *Radio Frequency Identification*, cujos princípios remontam à Segunda Guerra Mundial[42]. As tecnologias de radar e de rádio frequência utilizadas na Segunda Guerra Mundial

---

[38] KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. op. cit.
[39] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.
[40] MAGRANI, Eduardo. op. cit.
[41] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.
[42]FACCIONI FILHO, Mauro. **Internet das coisas**. Unisul Virtual, 2016. Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 08 abr. 2023.

continuaram a ser desenvolvidas após o seu fim, passando a ter aplicações comerciais, como, por exemplo, evitando roubos em lojas com etiquetas RFID[43].

A denominação de Internet das Coisas teria sido inicialmente trazida no ano de 1999, por Kevin Ashton (cofundador e diretor executivo do Auto - *ID Center*). O propósito dos estudos desenvolvidos pelo Auto - ID Center era de conectar as etiquetas de RFID, chamadas de "tags", com a internet, transformando a noção até então existente sobre a utilização desse sistema e oportunizando o uso da tecnologia para acompanhar toda a movimentação de cargas e de produtos. Essa ideia de relacionar o RFID com a conexão à internet trouxe uma visão inicial de Internet das Coisas[44].

Além da ideia de Kevin Ashton que abrangeria o termo, Neil Gershenfeld também trouxe a discussão sobre o tema em seu livro publicado em 1999, chamado "*When Things Start to Think*", onde descrevia "preocupações relacionadas às emoções e direitos civis em uma realidade onde objetos processam informação"[45] e mencionava que "as coisas começam a usar a Net"[46].

Em 2000, após a divulgação do termo, surgiu o primeiro eletrodoméstico que utilizava a interconexão com a internet na Coréia do Sul. De acordo com o presidente da LG (a marca de autoria da inovação) nos Estados Unidos, Simon Kang, os consumidores poderiam utilizar o aparelho não apenas como um refrigerador, mas como uma TV, rádio, aparelho da Web, videofone, quadro de avisos, calendário e câmera digital[47].

A partir de 2005, a discussão do tema ganhou maiores proporções em razão da atenção dada pelos governos e pelo início dos questionamentos quanto à privacidade e segurança das informações, tendo a IoT sido pauta, em 2005, da União Internacional de Telecomunicações, agência das Nações Unidas para as tecnologias

[43] FACCIONI FILHO, Mauro. op. cit.
[44] FACCIONI FILHO, Mauro. **Internet das coisas**. Unisul Virtual, 2016. Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 08 abr. 2023
[45] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.
[46] FACCIONI FILHO, Mauro. op. cit.
[47] SINGER, Talyta. op. cit.

da informação e da comunicação[48]. O relatório mencionava que "agora teremos conectividade para qualquer coisa" e que "as conexões se multiplicarão e criarão uma rede dinâmica de redes totalmente nova – uma Internet das Coisas"[49].

Ainda em 2005, foi lançado o Nabaztag, primeiro objeto inteligente, com forma similar a um coelho, que fora comercializado em escala. Ele possuía acesso à internet e podia ser programado para, por exemplo, ler e-mails, notícias e ver a previsão do tempo[50]. Em 2008, foi lançado o Patchube.com, plataforma que conecta dispositivos e fornece controle e armazenamento de dados em tempo real[51].

Em 2010, no Brasil, houve a implantação do COR - Centro de Operações do Rio, vinculado à prefeitura do Rio de Janeiro, que utiliza tecnologia de Cidades Inteligentes da IBM. Nele, um telão apresenta o mapa da cidade, com camadas de informação, e imagens de câmeras de vigilância, permitindo o acompanhamento do trânsito, condições climáticas e ocorrências[52].

Conforme indica Singer, em 2010, o número de objetos conectados à internet já havia superado o número de pessoas na Terra[53], e as evoluções desde então não pararam, de modo que já vislumbramos (e vislumbraremos ainda mais) o uso da IoT no nosso dia a dia.

Feitas as considerações iniciais sobre a origem da IoT, passa-se à análise mais destacada dos seus usos na sociedade atual.

3.2 CONCEITO(S) DE IOT E EXEMPLOS DE USO ATUAL

O primeiro obstáculo encontra-se na própria identificação do que vem a ser, especificamente, a Internet das Coisas, dado que seu conceito, por natureza, é flexível

[48] SINGER, Talyta. op. cit.
[49] Conforme extrai-se de: https://www.postscapes.com/iot-history/.
[50] SINGER, Talyta. op. cit.
[51] SINGER, Talyta. op. cit.
[52] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.
[53] Ibid.

e não possui um só significado amplamente aceito[54].

As diferentes definições costumam concordar, contudo, que a principal característica da IoT seria a conexão do mundo físico, que abrange as "coisas", com o mundo digital[55]. A União Internacional de Telecomunicações conceitua Internet das Coisas como uma infraestrutura para a sociedade da informação, que possibilita serviços avançados interconectando coisas com base nas tecnologias de informação e comunicação[56].

No Brasil, em 2019, foi criado o Plano Nacional de Internet das Coisas, instituído através do Decreto nº 9.854/19 e que possui como finalidade a implementação e o desenvolvimento, em nosso país, da Internet das Coisas, observadas, contudo, as diretrizes de segurança da informação e de proteção de dados pessoais[57]. Mencionado decreto define IoT como "a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação e comunicação existentes e nas suas evoluções, com interoperabilidade" [58].

Cabe indicar, também, que embora a IoT esteja amplamente ligada ao uso de internet na comunicação entre objetos, nem todos os objetos utilizam uma rede aberta, de modo que poderiam ser considerados objetos conectados a intranets[59].

Na visão de Belli, a Internet das Coisas pode ser compreendida como "uma rede que conecta objetos físicos identificados de maneira exclusiva a redes

---

[54] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023.
[55] Ibid.
[56] BELLI, Luca. op. cit.
[57] BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm. Acesso em: 08 abr. 2023.
[58] BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9854.htm. Acesso em: 08 abr. 2023.
[59] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023.

eletrônicas e softwares que permitem a comunicação e o processamento de dados coletados por meio das coisas"[60].

A melhor forma de visualizar o que é a Internet das Coisas é, em verdade, analisando alguns exemplos de sua aplicação. Nessa linha, temos relógios e óculos que permitem o acesso à internet, enviando e recebendo dados sobre o ambiente, a saúde e o bem-estar durante o exercício físico, como elevações de terreno, batimentos cardíacos, trajetos, etc[61], como a pulseira inteligente Nike+, FuelBand SE ou a FitBit.

Também, uma máscara que mede o movimento dos olhos, as ondas cerebrais e a tensão muscular, com o objetivo de garantir mais qualidade no descanso por meio da compreensão da melhor forma de acordar e o tempo ideal de sono, como é o caso da NeuroOn[62].

Já em uso no mercado, como outro exemplo de IoT, temos termostatos integrados ao smartphone, que não só ajustam a temperatura do local, mas também aprendem a rotina dos moradores. Detectores de fumaça, que acendem luzes coloridas, enviam mensagens de voz e notificações no smartphone. São exemplos de dispositivos criados pela Nest[63].

Do ponto de vista de utilização na administração pública, no Rio de Janeiro, há sensores, câmeras e camadas de informação que mostram trânsito e ocorrências diversas combinadas em tempo real no COR - Centro de Operações do Rio[64].

Outro exemplo de uso pelo poder público foi testado em Vitória da Conquista, onde etiquetas de radiofrequência foram implementadas aos uniformes dos alunos e monitoravam mais de 20 mil estudantes do ensino básico com o objetivo de registrar a entrada na escola e, em caso de falta, informar os pais[65].

---

[60] Ibid.

[61] DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, 2018. Disponível em: http://cm-kls-content.s3.amazonaws.com/LIVROS_UNOPAR_Digital.pdf. Acesso em: 08 abr. 2023.

[62] NG INFORMÁTICA.**11 exemplos provam que Internet das Coisas é capaz de mudar o mundo**. Disponível em: https://www.ngi.com.br/blog/11-exemplos-provam-que-internet-das-coisas-e-capaz-de-mudar-o-mundo/. Acesso em: 08 abr. 2023.

[63] Ibid.

[64] SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.

[65] Ibid.

Por fim, há ainda o exemplo do protótipo Mobii, que estava sendo desenvolvido pela Ford e pela Intel em 2014 e que pretendia equipar o carro com uma câmera que faria o reconhecimento do rosto do motorista, para oferecer informações sobre seu cotidiano, recomendar músicas, receber orientações para acionar o GPS e avisar o dono caso não reconhecesse o rosto, evitando furtos[66]. Não podemos esquecer, é claro, dos dispositivos Alexa e Amazon Echo, que também são exemplos dessa tecnologia.

A IoT já engloba bilhões de dispositivos inteligentes que são capazes de coletar, armazenar, processar e compartilhar elevadas quantidades de dados, não só sobre o funcionamento das coisas em si, mas também sobre o ambiente em que estão inseridas e sobre os indivíduos que as utilizam[67].

Dessa ideia de compartilharem-se dados com o intuito de apoiar outro propósito, que é essencial para que a IoT, acabam emergindo discussões sobre questões de ordem ética, política e prática[68].

Ademais, no contexto dos debates sobre segurança e do uso de IoT em Cidades Inteligentes, surgem relevantes indagações sobre a possibilidade de abuso e restrição à privacidade dos cidadãos[69].

A combinação de dados, base para o funcionamento da Internet das Coisas, torna-se, portanto, o foco central das discussões, sendo um desafio em relação à privacidade dos seus usuários[70].

---

[66] TECHTUDO. **Internet das Coisas**: o que é, como funciona e exemplos de uso, 2022. Disponível em: https://www.techtudo.com.br/noticias/2022/10/o-que-e-internet-das-coisas-veja-como-funciona-a-iot-e-exemplos-de-uso.ghtml. Acesso em: 08 abr. 2023.

[67] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023

[68] SANTOS, Carlos Cesar; SALES, Jefferson De Araujo. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.

[69] POETAS.IT. **IoT - Uma Estratégia para o Brasil** / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil, 2016. Disponível em: www.cesar.org.br/poetas.it/visionstatement. Acesso em: 09 abr. 2023.

[70] SANTOS, Carlos Cesar; SALES, Jefferson De Araujo. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.

3.3 IOT E CIDADES INTELIGENTES

A cidade vem se modificando para atender um ambiente atual de maior urbanização e para absorver as mudanças que o mundo digital tem proporcionado. O conceito de Cidades Inteligentes não é facilmente determinado, abrangendo um conjunto não homogêneo de projetos e de iniciativas[71].

As Cidades Inteligentes, ou *Smart Cities*, são, em uma definição simples, cidades conectadas, que usam a tecnologia para aprimorar a vida em sociedade, podendo servir para o monitoramento do trânsito, da segurança, apoio no acompanhamento do clima, dentre outros. O objetivo principal seria de agregar qualidade de vida e aperfeiçoar a eficiência administrativa na prestação de serviços públicos, a princípio, interconectando a cidade à rede mundial de computadores[72].

Em outras palavras, Cidades Inteligentes são cidades que usufruem da tecnologia com vistas a "prestar de forma mais eficiente os serviços urbanos, melhorar a qualidade de vida das pessoas e transformar a relação entre entidades locais, empresas e cidadãos"[73].

Não há um consenso sobre o conceito de Cidade Inteligente, entretanto, as definições indicam como elemento comum a tecnologia, se baseando, principalmente, no recolhimento de grande quantidade de dados, bem assim, no processamento e compartilhamento em tempo real destes dados como informação, para alcance dos objetivos da cidade[74].

Antonialli e Kira destacam que, no centro dos conceitos de Cidades Inteligentes, estaria "*o uso de tecnologias de informação e comunicação para a transformação de dinâmicas urbanas, tais como o planejamento urbano e territorial,*

---

[71] ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. **Revista brasileira de estudos urbanos e regionais**, v. 22, 2020. Disponível em: https://www.scielo.br/j/rbeur/a/QhMwqDCkcdDgrzVfcwVQgkr/abstract/?lang=pt. Acesso em: 18 jun. 2023.

[72] SANTIAGO, Mariana Ribeiro; PAYÃO, Jordana Viana. Internet das coisas e cidades inteligentes: tecnologia, inovação e o paradigma do desenvolvimento sustentável. **Revista de Direito da Cidade**, v. 10, n. 2, p. 787-805, 2018. Disponível em: https://www.e-publicacoes..php/rdc/article/view/31207. Acesso em: 18 jun. 2023.

[73] CUNHA, M. A; PRZEYBILOVICZ, E.; MACAYA, J. F. M; SANTOS, F. B. P. **Smart cities**: transformação digital de cidades. São Paulo: Programa Gestão Pública e Cidadania - PGPC, 2016. 161 p. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/18386. Acesso em 18 jun. 2023. p. 28.

[74] CUNHA, M. A; PRZEYBILOVICZ, E.; MACAYA, J. F. M; SANTOS, F. B. P. op. cit.

o engajamento e a participação cidadã, as políticas de mobilidade, habitação, entre outras"[75]. Para que isso seja possível, exige-se que a administração pública possa acessar e utilizar dados cada vez mais completos, permitindo ao gestor público que realize sua análise e otimize as políticas públicas[76].

Como exemplos de cidades que tiveram o seu desenvolvimento e planejamento aliados à conectividade, pode-se mencionar Songdo, na Coréia do Sul, e Masdar, em Abu Dhabi[77].

Uma das promessas da utilização da IoT, relacionada com o poder público, inclusive, é a oferta de maior eficácia no combate à criminalidade e maior capacidade de antecipação, prevenção e resposta para emergências ou situações de ameaça à ordem pública. Mirando esse objetivo, dados coletados por câmeras e a partir de dispositivos pessoais dos cidadãos são utilizados para promover o monitoramento e a vigilância onde há grande circulação de pessoas, como nos casos de megaeventos[78].

Ainda no que tange à segurança, sensores podem ser usados para reforçar a vigilância em edifícios públicos ou privados e a geolocalização pode servir para amplificar o monitoramento de fenômenos naturais, aperfeiçoando a prevenção e o resgate[79].

Verifica-se, portanto, que os sistemas de Internet das Coisas possuem potencial para aumentar a eficiência não só na segurança pública, mas em demais serviços de Cidades Inteligentes, como a saúde e os sistemas de gerenciamento

---

[75] ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. **Revista brasileira de estudos urbanos e regionais**, v. 22, 2020. Disponível em: https://www.scielo.br/j/rbeur/a/QhMwqDCkcdDgrzVfcwVQgkr/abstract/?lang=pt. Acesso em: 18 jun. 2023.

[76] Ibid.

[77] SANTIAGO, Mariana Ribeiro; PAYÃO, Jordana Viana. Internet das coisas e cidades inteligentes: tecnologia, inovação e o paradigma do desenvolvimento sustentável. **Revista de Direito da Cidade**, v. 10, n. 2, p. 787-805, 2018.

[78] POETAS.IT. **IoT - Uma Estratégia para o Brasil** / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das Coisas no Brasil, 2016. Disponível em: www.cesar.org.br/poetas.it/visionstatement. Acesso em: 09 abr. 2023.

[79] Ibid.

predial[80]. É nesse contexto que se apresenta um dos principais desafios: equilibrar a inovação, a busca da ordem pública e a manutenção da privacidade[81].

4 PRIVACIDADE X IOT E CIDADES INTELIGENTES

4.1 A QUESTÃO DA PRIVACIDADE NA ERA DIGITAL

A ideia de privacidade não é recente, contudo, mas sua conceituação abrangendo as características que vemos atualmente, se fez mais presente nas últimas décadas[82].

Dada a sua relevância, o direito à privacidade é reconhecido, na esfera internacional, mediante previsão no art. 12 da DUDH, que dispõe sobre o direito à proteção, indicando que "*ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência*", e o direito repressão de violações, dispondo que "*todo ser humano tem direito à proteção da lei contra tais interferências ou ataques*"[83].

Na esfera nacional, também é reconhecido como direito fundamental, na forma do art. 5º, X, da CF, que reconhece a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas, bem como assegura o direito à indenização em caso de violações[84].

Facchini Neto e Demoliner destacam que "*a tutela da privacidade destinava-se, quando da sua concepção originária, à proteção contra intromissões indesejadas na esfera pessoal do indivíduo*"[85].

---

[80] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023

[81] POETAS.IT. op. cit.

[82] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006. 448p. p. 91.

[83] ONU. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000139423. Acesso em: 25 ago. 2023.

[84] BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 ago. 2023.

[85] FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital: uma releitura do art. XII da Declaração Universal dos Direitos Humanos na sociedade do espetáculo. **Revista Internacional Consinter de Direito**, p. 119-140, 2019. p. 122.

Ingo Sarlet destaca que o direito à privacidade opera, no seu âmbito subjetivo, como um direito de defesa, garantindo a não intervenção de terceiros no âmbito de proteção, e também como expressão da liberdade pessoal e do direito da pessoa dispor das informações atinentes à sua vida privada[86].

Do seu âmbito objetivo, entretanto, decorre o dever de proteção estatal contra intervenções, apresentando-se como garantia de fruição da privacidade como um direito reconhecido pelo ordenamento jurídico pátrio[87].

Ocorre que as discussões atuais no que toca ao direito à privacidade não são as mesmas de anos anteriores. Os avanços tecnológicos, a globalização, o aumento de fluxo de dados, dentre outros, acabaram influenciando a organização social, exigindo uma readequação da sociedade[88] e do próprio direito.

No que toca ao direito, os impactos são tamanhos que, atualmente, tem se falado na existência de um processo de digitalização dos direitos fundamentais (mas não só destes), promovendo a sua releitura diante do contexto social e jurídico atual[89].

O direito à privacidade restou afetado pelas inovações tecnológicas que permitiram o desenvolvimento de novas formas de lesionar a esfera privada e que requerem novas respostas, lastreadas na releitura ou reformulação desse direito[90].

Em linha com o entendimento de Fernando Machado, "*a construção de um direito à privacidade sempre foi marcada pelas possiblidades e implicações decorrentes do desenvolvimento de novas tecnologias*" e, atualmente, as formulações mais atuais do direito à privacidade, o caracterizam como o direito de ter o controle do fluxo de informações pessoais, verificando-se "*uma tentativa de*

---

[86] SARLET, Ingo Wolfgang. Direitos fundamentais em espécie. In: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de direito constitucional. 10. ed. São Paulo: Saraiva Educação, 2021a. p. 178-367. p. 200-201.
[87] Ibid. p. 200-201.
[88] MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação**: Profiling e risco de discriminação. Dissertação (Mestrado em Direito). Escola de Direito. Pontifícia Universidade Católica do Rio Grande do Sul. p. 194. 2018. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/8002/5/DIS_FERNANDO_INGLEZ_DE_SOUZA_MACHADO_COMPLETO.pdf. Acesso em: 25 ago. 2023. p. 14.
[89] SARLET, Ingo Wolfgang. Fundamentos constitucionais: O direito fundamental à proteção de dados. In: BIONI, Bruno; DONEDA, Danilo. et. al. (coord.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021b. p. 40-78. p. 40.
[90] MACHADO, Fernando Inglez de Souza. op. cit. p. 15.

tutela da esfera privada do indivíduo e de sua própria personalidade frente a ameaças que os avanços tecnológicos ensejam"[91].

Bolesina e Garvasoni afirmam que o direito à privacidade foi um dos mais impactados pelas transformações tecnológicas, tendo passado de uma perspectiva mais intimista que indicava ser este um direito de estar só ou de não ter perturbações no seu espaço privado, para uma visão mais ampla que abrange faculdades relacionadas com as esferas existencial e patrimonial, seja em espaços físicos, seja em espaços virtuais[92].

As discussões sobre a proteção da privacidade e as evoluções tecnológicas têm andado juntas ao longo da história e, seguindo esse raciocínio, espera-se que não será diferente se tratando de IoT[93].

4.2 PROBLEMATICA DA PROTEÇÃO DA PRIVACIDADE X IOT E CIDADES INTELIGENTES

Como explicado anteriormente, a Internet das Coisas consiste, de forma ampla, em objetos que através de conexão – com a internet ou intranet – enviam dados, trocando informações entre si.

Se por um lado a interconexão entre diversos objetos pode significar um ganho de produtividade e trazer diversos benefícios aos seus consumidores, por outro, esses objetos inteligentes, que nos acompanham rotineiramente, coletam, transmitem, armazenam e compartilham inúmeros dados, muitos deles particulares e até íntimos[94].

---

[91] MACHADO, Fernando Inglez de Souza. op. cit.

[92] BOLESINA, I.; GERVASONI, T. A. A proteção do direito fundamental à privacidade na era digital e a responsabilidade civil por violação do direito à extimidade. **Novos Estudos Jurídicos**, Itajaí, SC, v. 27, n. 1, p. 87–109, 2022. DOI: 10.14210/nej.v27n1.p87-109. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/16093. Acesso em: 25 ago. 2023.

[93] DIAS, Carlos André Ferreira. **A Privacidade na era da Internet das Coisas**: direitos de personalidades e proteção de dados. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2019. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/140094/2/536105.pdf. Acesso em: 25 ago. 2023.

[94] MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em: https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.

O número de sensores tem aumentado e, em um mundo amplamente conectado, torna-se imperiosa a modificação nos paradigmas da privacidade, até então vigentes. Como destaca Dias, na sociedade atual surge facilmente o questionamento sobre a existência ou não de privacidade "*quando uma infraestrutura de milhares de milhões de sensores integrados em dispositivos do quotidiano de qualquer pessoa são capazes de registar, tratar, armazenar e transferir dados a todo o momento e de forma contínua*"[95].

No cenário atual, com o aumento exponencial do uso e o desenvolvimento de novos produtos com a tecnologia, é necessário manter a atenção para os riscos de violações de privacidade e de segurança dos usuários[96] e, também, para com a segurança pública nos casos de utilização de sistemas com IoT pelo governo[97].

A possibilidade de hackeamento, controle remoto e manipulação de dispositivos pode ocasionar lesão não só à privacidade dos indivíduos, por violação do domicílio, correspondência, vida familiar, mas também à segurança pessoal[98]. Tais lesões podem se tornar ainda mais latentes se considerarmos que a maioria das pessoas pode não possuir conhecimento de que determinados objetos (até brinquedos), que estão em ambientes familiares ou de trabalho, coletam e compartilham dados[99].

Belli destaca estudo feito pela Northeastern em conjunto com o Imperial College London, que analisou as atividades de compartilhamento de dados de 81 objetos inteligentes que podem ser encontrados, usualmente, em residências, como SmartTVs, campainhas conectadas, alto-falantes, dentre outros. O estudo revelou que 72 dispositivos coletavam dados de forma desproporcional, além do necessário

---

[95] DIAS, Carlos André Ferreira. **A Privacidade na era da Internet das Coisas**: direitos de personalidades e proteção de dados. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2019. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/140094/2/536105.pdf. Acesso em: 25 ago. 2023. p. 31.
[96] MAGRANI, Eduardo. op. cit.
[97] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023.
[98] Ibid.
[99] BELLI, Luca. op. cit.

para o objeto, como informações pessoais, endereços de IP, dados de localização, dentre outros, e compartilhavam as informações com terceiros[100].

Marques e Lemos destacam que diversos problemas de privacidade, segurança e vigilância podem aparecer "desde a definição do tipo de dado captado pelos sensores, passando por suas formas de circulação e armazenamento, pelo compartilhamento com empresa parceira, pela relação com outros dados em banco de dados"[101], dentre outros.

Os problemas envolvendo privacidade possuem ao menos três diferentes perspectivas a serem pensadas: violações pelo governo, violações por empresas e acesso por pessoas mal-intencionadas. É impossível tratar das inovações que a Internet das Coisas propicia sem vislumbrar também os riscos de sua utilização, ainda mais quando tratamos de aplicações que permitem a localização de pessoas, o acesso a informações da vida privada, vislumbrar dados de saúde, dentre outros[102].

Questões envolvendo a privacidade são complexas de resolver e tendem a tornar-se ainda mais complicadas com as evoluções tecnológicas experimentadas[103], bem assim, quando seu uso é implementado no serviço público.

Até porque, se a implementação de Cidades Inteligentes exigirá a criação de bancos de dados completos e complexos, que armazenem registros sobre os cidadãos, como podemos possibilitar os avanços nessa seara sem ameaçar a privacidade individual [104]?

---

[100] BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023.
[101] MARQUES, Daniel; LEMOS, André. **Sensibilidade Performativa e Privacidade na Internet das Coisas**. Disponível em: https://lavits.org/wp-content/uploads/2018/04/43-Daniel-Marques-e-Andr%C3%A9-Lemos.pdf. Acesso em: 09 abr. 2023.
[102] SANTOS, Carlos Cesar; SALES, Jefferson De Araujo. O desafio da privacidade na internet das coisas. GESTÃO. Org, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.
[103] SANTOS, Carlos Cesar; SALES, Jefferson De Araujo. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.
[104] ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. **Revista brasileira de estudos urbanos e regionais**, v. 22, 2020. Disponível em: https://www.scielo.br/j/rbeur/a/QhMwqDCkcdDgrzVfcwVQgkr/abstract/?lang=pt. Acesso em: 18 jun. 2023

Câmara e Ramiro informam que, "*no momento em que o cidadão interage com uma Cidade Inteligente, ele está sujeito à vigilância, seja estatal ou empresarial*"[105].

Diante disso, o desenvolvimento de Cidades Inteligentes, dado o potencial de lesão à privacidade e à proteção de dados, deve ser realizado com atenção aos direitos constitucionalmente garantidos, levando-os em consideração desde o planejamento inicial, nas soluções para o consentimento do usuário e também na manutenção da transparência no que toca à coleta, uso e armazenamento das informações, modo a proteger o cidadão e buscando preservar a sua autonomia.

5 CONSIDERAÇÕES FINAIS

Em linha com o exposto no presente trabalho, a Internet, que nos seus primeiros anos de uso servia, sinteticamente, para realizar a conexão entre pessoas, passou a ser utilizada, adicionalmente, para conectar dispositivos e máquinas, por redes sem fio ou com fio, através do que ficou denominado como Internet das Coisas.

Essa ideia de IoT está diretamente vinculada com a evolução da própria Internet, que hoje possui o objetivo, também, de extrair conteúdos, captar informações e promover o processamento, compreensão e análise de dados.

Observou-se que não há um consenso sobre o conceito de IoT, mas há pontos de similaridade entre as conceituações, destacando-se, principalmente, a possibilidade de conexão do mundo físico, que abrange as "coisas", com o mundo digital.

Ademais, os debates sobre a privacidade diante da evolução tecnológica não são poucos e tem, inclusive, se intensificado concomitantemente ao próprio desenvolvimento e implementação de novas tecnologias. Não seria diferente se tratando de IoT.

Verificou-se que as discussões se intensificam ainda mais quando o tema é a utilização de IoT pelo poder público e o desenvolvimento de Cidades Inteligentes,

---

[105] RAMIRO, André; CÂMARA, Amália. **A Privacidade Em Um Cenário Pansensitível De Internet Das Coisas & Cidades Inteligentes**. 14 a 16 de Dezembro de 2017–Escola de Comunicações e Artes da Universidade de São Paulo, 2017. p. 363.

situação em que surgem relevantes indagações sobre a possibilidade de abuso e restrição à privacidade dos cidadãos.

Por fim, concluiu-se que o uso de Internet das Coisas e o desenvolvimento de Cidades Inteligentes apresenta potencial de lesionar e/ou causar impactos negativos na esfera de proteção da privacidade dos cidadãos, principalmente se o desenvolvimento do uso da tecnologia pelo poder público se der sem prévia atenção aos riscos para a privacidade.

REFERÊNCIAS

ANTONIALLI, Dennys Marcelo; KIRA, Beatriz. Planejamento urbano do futuro, dados do presente: a proteção da privacidade no contexto das cidades inteligentes. **Revista brasileira de estudos urbanos e regionais**, v. 22, 2020. Disponível em: https://www.scielo.br/j/rbeur/a/QhMwqDCkcdDgrzVfcwVQgkr/abstract/?lang=pt. Acesso em: 18 jun. 2023.

BELLI, Luca. Uma perspectiva de Direitos Humanos para decriptar a ascensão da Internet das Coisas (IoT). **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 13, n. 41, p. 157-181, 2019. Disponível em: https://dfj.emnuvens.com.br/dfj/article/view/775. Acesso em 08 abr. 2023.

BOLESINA, I.; GERVASONI, T. A. A proteção do direito fundamental à privacidade na era digital e a responsabilidade civil por violação do direito à extimidade. **Novos Estudos Jurídicos**, Itajaí, SC, v. 27, n. 1, p. 87–109, 2022. DOI: 10.14210/nej.v27n1.p87-109. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/16093. Acesso em: 25 ago. 2023.

BRASIL. **Constituição (1988)**. Constituição da República Federativa do Brasil. Brasília, DF. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 ago. 2023.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019 2022/2019/decreto/d9854.htm. Acesso em: 08 abr. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 abr. 2023.

CUNHA, Maria Alexandra; PRZEYBILOVICZ, Erico; MACAYA, Javiera Fernanda Medina; SANTOS, Fernando Burgos Pimentel dos. **Smart cities**: transformação digital de cidades. São Paulo: Programa Gestão Pública e Cidadania - PGPC, 2016. 161 p. Disponível em: https://bibliotecadigital.fgv.br/dspace/handle/10438/18386. Acesso em 18 jun. 2023.

DECARLI, Gian Carlo. **História e evolução da internet**. Tendências do marketing digital, 2018. Disponível em: http://cm-klscontent.s3.amazonaws.com/LIVROS_UNOPAR_AEDU/Tend%C3%AAncias%20Do%20Marketing%20Digital.pdf. Acesso em: 08 abr. 2023.

DIAS, Carlos André Ferreira. **A Privacidade na era da Internet das Coisas**: direitos de personalidades e proteção de dados. Dissertação (Mestrado em Ciências Jurídico-civilísticas) Faculdade de Direito da Universidade do Porto. Porto, 2019. Disponível em: https://repositorio-aberto.up.pt/bitstream/10216/140094/2/536105.pdf. Acesso em: 25 ago. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. 448p. p. 91.

FACCHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à privacidade na era digital: uma releitura do art. XII da Declaração Universal dos Direitos Humanos na sociedade do espetáculo. **Revista Internacional Consinter de Direito**, p. 119-140, 2019.

FACCIONI FILHO, Mauro. **Internet das coisas**. Unisul Virtual, 2016. Disponível em: https://www.researchgate.net/profile/Mauro-Fazion-Filho/publication/319881659_Internet_das_Coisas_Internet_of_Things/links/59c038d5458515e9cfd54ff9/Internet-das-Coisas-Internet-of-Things.pdf. Acesso em: 08 abr. 2023.

GIBBS, Samuel. **Samsung's voice-recording smart TVs breach privacy law, campaigners claim.** The Guardian. Disponível em: https://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim. Acesso em: 09 abr. 2023.

GUO, Eileen. **A Roomba recorded a woman on the toilet. How did screenshots end up on Facebook?**. Disponível em: https://www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/. Acesso em: 09 abr. 2023.

HERN, Alex. **Roomba maker may share maps of users' homes with Google, Amazon or Apple.** Disponível em: https://www.theguardian.com/technology/2017/jul/25/roomba-maker-could-

share-maps-users-homes-google-amazon-apple-irobot-robot-vacuum. Acesso em: 09 abr. 2023.

KLEIN, Júlia Schroeder Bald; ADOLFO, Luiz Gonzaga Silva. A Web 4.0 e os Riscos à Democracia. **Revista Em Tempo**, [S.l.], v. 20, n. 1, nov. 2020. ISSN 1984-7858. Disponível em: <https://revista.univem.edu.br/emtempo/article/view/3132>. Acesso em: 08 abr. 2023.

LANDAU, Susan. **What Was Samsung Thinking**?. IEEE Security & Privacy, vol. 13, nº. 3, pp. 3-4, May-June, 2015, doi: 10.1109/MSP.2015.63. Disponível em: https://ieeexplore.ieee.org/document/7118090. Acesso em: 09 abr. 2023.

LINS, Bernardo Felipe Estellita. A evolução da Internet: uma perspectiva histórica. **Cadernos Aslegis**, v. 48, p. 11-45, 2013. Disponível em: http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf. Acesso em: 08 abr. 2023.

MACHADO, Fernando Inglez de Souza. **Privacidade e proteção de dados pessoais na sociedade da informação**: Pprofiling e risco de discriminação. Dissertação (Mestrado em Direito). Escola de Direito. Pontifícia Universidade Católica do Rio Grande do Sul. p. 194. 2018. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/8002/5/DIS_FERNANDO_INGLEZ_DE_SOUZA_MACHADO_COMPLETO.pdf. Acesso em: 25 ago. 2023.

MAGRANI, Eduardo. **A internet das coisas**. Rio de Janeiro: FGV Editora, 2018. Disponível em:https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/23898/A%20internet%20das%20coisas.pdf. Acesso em: 28 mar. 2023.

MARQUES, Daniel; LEMOS, André. **Sensibilidade Performativa e Privacidade na Internet das Coisas**. Disponível em: https://lavits.org/wp-content/uploads/2018/04/43-Daniel-Marques-e-Andr%C3%A9-Lemos.pdf. Acesso em: 09 abr. 2023.

NG INFORMÁTICA.**11 exemplos provam que Internet das Coisas é capaz de mudar o mundo**. Disponível em: https://www.ngi.com.br/blog/11-exemplos-provam-que-internet-das-coisas-e-capaz-de-mudar-o-mundo/. Acesso em: 08 abr. 2023.

OLHAR DIGITAL. **Hackers invadem sistema de casa e infernizam moradores**. 2019. Disponível em: https://olhardigital.com.br/2019/09/24/seguranca/hackers-invadem-sistema-de-casa-e-infernizam-moradores/. Acesso em: 09 abr. 2023.

ONU. **Declaração Universal dos Direitos Humanos**. 1948. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000139423. Acesso em: 25 ago. 2023.

POETAS.IT. **IoT - Uma Estratégia para o Brasil** / Consolidação de uma visão unificada para orientação e proposição de políticas públicas sobre Internet das

Coisas no Brasil, 2016. Disponível em: www.cesar.org.br/poetas.it/visionstatement. Acesso em: 09 abr. 2023.

PRADO, Jean. **Brinquedo conectado à internet vaza dados de crianças**. Tecnoblog. 2017. Disponível em: https://tecnoblog.net/noticias/2017/03/03/brinquedo-conectado vazamento-dados-criancas/. Acesso em: 09 abr. 2023.

RAMIRO, André; CÂMARA, Amália. **A Privacidade Em Um Cenário Pansensitível De Internet Das Coisas & Cidades Inteligentes**. 14 a 16 de Dezembro de 2017–Escola de Comunicações e Artes da Universidade de São Paulo, 2017.

ROCHA, G. C da; SOUZA FILHO, V. B de. Da guerra às emoções: história da internet e o controverso surgimento do Facebook. **Encontro Regional Norte de História da Mídia**, v. 4, 2016. Disponível em: http://www.alcarnorte.com.br/wp-content/uploads/alcar2016_da_guerra_as_emocoes_historia_da_internet_e_o_controverso_surgimento_do_facebook.pdf. Acesso em: 08 abr. 2023.

SANTIAGO, Mariana Ribeiro; PAYÃO, Jordana Viana. Internet das coisas e cidades inteligentes: tecnologia, inovação e o paradigma do desenvolvimento sustentável. **Revista de Direito da Cidade**, v. 10, n. 2, p. 787-805, 2018. Disponível em: https://www.e-publicacoes.uerj.br/index.php/rdc/article/view/31207. Acesso em: 18 jun. 2023.

SANTOS, Carlos Cesar; SALES, Jefferson de Araujo. O desafio da privacidade na internet das coisas. **GESTÃO. Org**, v. 13, n. 4, p. 282-290, 2015. Disponível em: https://dialnet.unirioja.es/servlet/articulo?codigo=7653186. Acesso em: 08 abr. 2023.

SARLET, Ingo Wolfgang. Direitos fundamentais em espécie. In: SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. **Curso de direito constitucional**. 10. ed. São Paulo: Saraiva Educação, 2021a. p. 178-367.

SARLET, Ingo Wolfgang. Fundamentos constitucionais: O direito fundamental à proteção de dados. In: BIONI, Bruno; DONEDA, Danilo. et. al. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021b. p. 40-78.

SINGER, Talyta. Tudo conectado: conceitos e representações da internet das coisas. **Simpósio em tecnologias digitais e sociabilidade**, v. 2, p. 1-15, 2012. Disponível em: http://www.simsocial2012.ufba.br/modulos/submissao/Upload/44965.pdf. Acesso em: 08 abr. 2023.

TECHTUDO. **Internet das Coisas**: o que é, como funciona e exemplos de uso, 2022. Disponível em: https://www.techtudo.com.br/noticias/2022/10/o-que-e-internet-das-coisas-veja-como-funciona-a-iot-e-exemplos-de-uso.ghtml. Acesso em: 08 abr. 2023.

VIGGIANO, Giuliana. **Brinquedos hackeados conseguiram "ouvir" mensagens de crianças.** Revista Galileu. 2017. Disponível em: https://revistagalileu.globo.com/Tecnologia/noticia/2017/06/brinquedos-hackeados-conseguiram-ouvir-mensagens-de-criancas.html. Acesso em: 09 abr. 2023.

11. A LEI GERAL DE PROTEÇÃO DE DADOS EM CONSULTÓRIOS MÉDICOS

 https://doi.org/10.36592/9786554600712-11

Taiane Meirelles Alfonsin[1]

SUMÁRIO

1. Introdução. 2 Principais pontos da lei geral de proteção de dados na área da saúde. 3. Diretrizes para adequação da LGPD em consultórios médicos. 4.Conclusão. 5. Referências.

RESUMO

Este artigo se propõe a ser uma fonte preliminar de ponderações e reflexões dos impactos da implementação da Lei Geral de Proteção de dados em consultórios médicos, a qual tem importância significativa, pois estes lidam com informações sensíveis de pacientes. Tais clínicas precisam ter um cuidado especial no armazenamento, coleta e compartilhamento desses dados para estar em conformidade com a LGPD. O não cumprimento da LGPD pode resultar em multas pesadas e danos à reputação da clínica. Portanto, é crucial adotar práticas em conformidade com a lei. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.[2] Deste modo, em agosto de 2018 foi sancionada a Lei nº 13.709, popularmente conhecida como Lei Geral de Proteção de Dados Pessoais, ou simplesmente LGPD, para proteger os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade de cada indivíduo. Assim, não cumprir essas obrigações não é mais uma opção devido às consequências legais significativas e danos à reputação. Portanto, é vital para qualquer consultório médico possuir um plano de resposta a incidentes de violação de dados alinhado com as exigências da LGPD. A conformidade com a LGPD deve ser vista não apenas como uma obrigação legal, mas também uma forma de estabelecer confiança junto aos pacientes ao garantir a integridade e confidencialidade das suas informações de saúde.
Palavras-chave: Lei Geral de Proteção de Dados; dados sensíveis; consultório médico.

---

[1] Bacharel em Direito pela Uniritter em 2008, Mestre em Direito pela Unisinos, Especialista em Direito Civil e Processo Civil, Advogada militante na área de recuperação de crédito, direito imobiliário e previdência privada. Membro da Comissão Especial de Compliance da OAB/RS. E-mail: taiane.alfonsin@bothomeadv.com.br

[2] CONSUMERS INTERNATIONAL. **Consumers International**: Strategy. [*S. l.*]: Consumers International, 2018. Disponível em: https://www.consumersinternational.org/media/155232/strategy-eng.pdf. Acesso em: 7 jul. 2021. p. 4.

ABSTRACT

This article proposes to be a preliminary source of considerations and reflections on the impacts of the General Data Protection Law on medical offices, which have a significant impact, as they deal with sensitive patient information. These clinics need to take special care in storing, collecting and sharing this data in order to comply with the GDPR. Non-compliance with the LGPD can result in heavy fines and damage to the clinic's reputation. It is therefore crucial to adopt practices that comply with the law.In this context, many countries have adopted new data protection rules or modernized the ones they already had, such as South Korea, Chile, Thailand, India, Indonesia and Brazil. Currently, there are more than one hundred countries with regulatory frameworks for the protection of personal data around the world. Thus, in August 2018, Law No. 13,709, popularly known as the General Law for the Protection of Personal Data or simply LGPD, was enacted to protect the fundamental rights of freedom and privacy and the free formation of the personality of each individual. Therefore, failure to comply with these obligations can lead to significant legal consequences and reputational damage. Therefore, it is vital for any medical practice to have a data breach incident response plan aligned with the requirements of the GDPR. Compliance with the LGPD is not only a legal obligation, but also a way to establish trust with patients and ensure the integrity and confidentiality of their health information.
Keywords: General Data Protection Law. Sensitive Data. Doctor's office.

1 INTRODUÇÃO

O surgimento da Lei Geral de Proteção de Dados não adveio de um capricho ou de um preciosismo legal; havia uma necessidade imperativa de sistematizar a proteção dos dados pessoais e, no circuito da área da saúde, é um tema ainda mais complexo que requer uma abordagem detalhada e cuidadosa para garantir a conformidade e proteger os direitos dos indivíduos, pois sem segredo não há confiança; sem confiança não há medicina. Assim, com a entrada em vigor da lei no Brasil em setembro de 2020, foram estabelecidas regras para o tratamento de dados pessoais, inclusive em consultórios médicos. Desta forma, este artigo destaca os principais pontos da LGPD e como os consultórios médicos podem se adequar à nova legislação.

A referida lei estabelece regras para o coleta, armazenamento, tratamento e compartilhamento de dados pessoais, afetando todas as empresas e instituições que lidam com informações pessoais, incluindo consultórios médicos, escopo do presente artigo. Os consultórios médicos coletam e armazenam uma grande

quantidade de dados pessoais e sensíveis, como histórico médico/prontuários, exames, fotografias, informações de contato, anamnese, prontuários eletrônicos, receitas ou qualquer outro registro que contenha dados pessoais. A LGPD exige que esses dados sejam tratados de maneira segura e transparente.

O direito à privacidade surgiu com a publicação do artigo "The right to privacy", escrito por Samuel Warren e Louis Brandeis, publicado em 1890 na já citada Harvard Law Review, que defende a existência de um direito de estar e de ficar sozinho (right to be let alone).[3]

Uma das principais questões que permeia entre pessoas é a privacidade (ou ausência dela), ainda mais em uma sociedade hiper conectada, por isso a importância do presente estudo. Além disso, definir quais diretrizes são necessárias para implementação da LGPD em consultórios médicos é fundamental para evitar as consequências jurídicas e pecuniárias de um possível descumprimento. Não restam dúvidas quanto à relevância do tema e, por conseguinte, da necessidade impositiva das clínicas médicas de se adequarem as exigências implementadas pela nova legislação.

Assim clínicas, hospitais, operadores de saúde, com o advento da LGPD não serão proibidos de tratar dados de seus pacientes e colaborardes, mas deverão se adequar aos preceitos elencados pela lei.

2 PRINCIPAIS PONTOS DA LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

A entrada em vigor da LGPD afetou a rotina das empresas, independente do setor em que atuam assim para evitar futuras consequências jurídicas, os consultórios médicos, que coletam e armazenam uma grande quantidade de dados

[3] "Devemos, portanto, concluir que os direitos assim protegidos, qualquer que seja sua natureza exata, não são direitos decorrentes de contrato ou de confiança especial, mas são direitos contra o mundo; e, como dito acima, o princípio que foi aplicado para proteger esses direitos não é, na realidade, o princípio da propriedade privada, a menos que esse mundo seja usado em um sentido extenso e incomum. O princípio que protege os escritos pessoais e quaisquer outras produções do intelecto ou das emoções é o direito à privacidade, e a lei não tem nenhum princípio novo a formular quando estende essa proteção à aparência pessoal, ditos, atos e à relação pessoal, doméstica ou outro." (WARREN, Samuel D.; BRANDEIS, Louis D. Right to Privacy. **Harvard Law Review**, Boston, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/ cs5436/warren-brandeis.pdf?. Acesso em: 16 jun. 2021. p. 213.)

pessoais sensíveis devem se adequarem a fim de evitar prejuízos de ordem financeira, danos à reputação e erosão da confiança do paciente. Por isso, a LGPD exige que esses dados sejam tratados de maneira segura e transparente. O Artigo 5º da Lei Geral de Proteção de Dados (LGPD), inciso II[4], define o que são dados sensíveis. Segundo a lei, dados sensíveis são aqueles sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O tratamento desses tipos de dados é mais rigoroso sob a LGPD e, na maioria dos casos, só pode ser realizado com o consentimento explícito do titular, salvo algumas exceções previstas em lei. A LGPD estabelece um conjunto de condições especiais para o tratamento de dados sensíveis, dada a natureza dessas informações e o risco de discriminação ou outros prejuízos para o titular. Portanto, as empresas e instituições que lidam com dados sensíveis, como consultórios médicos, devem adotar medidas adicionais para garantir a conformidade com a lei.

Nesse intuito, temos ainda outro ponto importante que diz respeito ao tempo de armazenamento dos dados dos pacientes no consultório médico, segundo a Lei, a motivação/finalidade do armazenamento deve ser minimamente apresentada quando da coleta do dado. Em outras palavras, o período de armazenamento dos dados deve respeitar a autorização/consentimento do titular do dado e a concretização da finalidade da coleta.

A título exemplificativo, foi analisada a Política de Privacidade do Hospital Albert Eisntein, sendo que na referida política é definida quais dados são coletados e como são protegidos em toda atividade de tratamento (coleta, registro, armazenamento, uso, compartilhamento, enriquecimento e eliminação)

> Além disso, para assegurar e resguardar a vida o Einstein poderá tratar os dados pessoais sensíveis de seus usuários, com base na tutela da saúde, assim como para as finalidades previstas no consentimento informado quando aplicável, tais

[4] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 set. 2023.

> como procedimentos realizados por profissionais da saúde e serviços de saúde, comunicações relevantes para a promoção da sua saúde, pesquisas de satisfação para melhoria de nossos serviços, entre outros.[5]

Quanto ao prazo, o referido hospital assim define em sua Política:

> Os dados são conservados pelo período estritamente necessário para cada uma das finalidades descritas acima e/ou de acordo com prazos legais vigentes. Em caso de litígio pendente, os dados podem ser conservados até trânsito em julgado da decisão[6]

Porém, na Medicina os prontuários fisico ou digital devem ser obrigatoriamente serem guardados por 20 anos, determinação essa ressalvada pela LGPD Art. 16 - I, que prevê a conservação de dados para obrigação legal.[7]

Outro exemplo prático, são as conversas por WhatsApp, onde a LGPD deve também ser respeitada, pois circulam nesses grupos informações clínicas de pacientes que não podem ser reveladas, bem como o quadro de saúde dos mesmos, a não ser de forma anonimizado[8].

Assim, denota-se que a a política de dados é fundamental para estabelecer as regras e diretrizes que governam a coleta, armazenamento, processamento e compartilhamento de dados dentro de uma organização.

A Lei Geral de Proteção de Dados (LGPD) tem implicações significativas para a área da saúde no Brasil, posto que os dados de saúde são considerados "dados sensíveis", exigindo maior rigor no seu tratamento. Ademais, antes de coletar ou processar dados de saúde, é fundamental obter o consentimento explícito do titular.

---

[5] TERMOS de uso e política de privacidade. *In:* HOSPITAL Israelita Albert Einstein. São Paulo, 2022. Disponível em: https://www.einstein.br/sobre-einstein/politicas-site. Acesso em: 07 set. 2023.

[6] TERMOS de uso e política de privacidade. *In:* HOSPITAL Israelita Albert Einstein. São Paulo, 2022. Disponível em: https://www.einstein.br/sobre-einstein/politicas-site. Acesso em: 07 set. 2023.

[7] BARROS JÚNIOR, Edmilson de Almeida. **Direito Médico**. Brasil: Haikai Editora, 2022.

[8] Art. 12. Os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido. (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 set. 2023.)

Este consentimento deve ser específico e informado.[9] Assim, dada a sensibilidade dos dados de saúde, medidas rigorosas de segurança devem ser implementadas, incluindo criptografia e sistemas de controle de acesso. A LGPD restringe o compartilhamento de dados sensíveis, qualquer compartilhamento deve ser feito com o consentimento do titular e somente para os fins para os quais os dados foram coletados. Os titulares têm o direito de solicitar a portabilidade de seus dados para outros prestadores de serviços de saúde, sujeito a algumas condições, conforme preceitua o artigo 18, inciso V da Lei Gera de Proteção de Dados. Ainda, é direito do titular acessar, corrigir, excluir ou bloquear seus dados. Os estabelecimentos de saúde devem facilitar esses processos.

A depender do tamanho do consultório médico, pode ser fazer necessário a nomeação de um *Data Protection Officer* (DPO), para garantir a conformidade com a LGPD. O pessoal que lida com dados de saúde deve ser treinado sobre as melhores práticas e conformidade com a LGPD. Muito mais que apenas impedir o acesso indesejado às informações pessoais, a LGPD preocupa-se também, conforme previsto em seu art. 2º, inciso II, à autodeterminação informativa como fundamento, embora não enunciado na Constituição Federal, pode ser visualizado no conjunto dos princípios e dos seu outros direitos constitucionais expressos, nada mais é que ter a faculdade de o particular determinar e controlar a utilização dos seus dados pessoais.

Hoje, ocorrendo um incidente de segurança - como um problema em um software, a existência de um ataque cibernético, o acesso de um terceiro não autorizado, um extravio de um prontuário físico ou o uso de dados sensíveis para aplicação de golpes - o hospital ou clínica médica deverá comunicar rapidamente à ANPD (mesmo que as informações de saúde ainda não tiverem sido violadas) além de ser obrigado a indicar quais foram as condutas que adotou (técnicas e

---

[9] Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas [...] (BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 set. 2023.)

administrativas) para garantir a privacidade do titular, sem prejuízo dos demais deveres elencados na lei.

Cumpra ressaltar, que a Agência Nacional de Proteção de Dados (ANPD) já aplicou sua primeira penalidade administrativa pelo descumprimento da LGPD. Surpreendentemente, a primeira penalidade aplicada foi direcionada a uma microempresa.[10] A LGPD foi aprovada em 2018 e entrou em vigor em setembro de 2020. Porém, as sanções previstas na lei tiveram um período maior para adaptação e passaram a valer em agosto de 2021, mas só foram regulamentadas no último mês de fevereiro. A partir de agora, a ANPD passa a efetivamente ter todas as condições necessárias para a aplicação das sanções previstas na LGPD, de modo que a fiscalização de conformidade com a legislação ganha outro patamar. Até então, diversas empresas tinham deixado seus projetos de adequação à norma de lado, enquanto não havia sequer possibilidade concreta de serem sancionadas. Com a edição do regulamento, a conduta do mercado em relação à proteção de dados pessoais deve mudar.[11]

A aplicação da LGPD na área da saúde é particularmente importante, onde existem diversos aspectos centrais, tais como, a sensibilidade dos dados, o que significa que requerem um nível mais alto de proteção; a importância do consentimento: enquanto a "tutela da saúde" pode ser usada como uma base legal para processar dados em certos casos, o consentimento explícito do paciente é muitas vezes preferível e, em alguns casos, necessário; a segurança, sendo primordial que as instituições de saúde sejam obrigadas a adotar medidas de segurança robustas para proteger os dados contra acessos não autorizados, perdas e vazamentos; o direito do acesso e portabilidade: os pacientes têm o direito de acessar seus próprios dados de saúde e podem solicitar a transferência desses dados para outros prestadores de serviços de saúde; o princípio da transparência: os pacientes devem ser informados sobre como seus dados serão coletados,

---

[10] ANPD aplica a primeira multa por descumprimento à LGPD. *In:* GOV.BR. Ministério da Justiça e Segurança Pública. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 07 set. 2023.

[11] SANTOS, Rafa. Regulamento avança na aplicação da LGPD ao disciplinar dosimetria das penas. **Consultor Jurídico**, São Paulo, 27 fev. 2023. Disponível em: https://www.conjur.com.br/2023-fev-27/regulamento-avanca-aplicacao-lgpd-disciplinar-penas. Acesso em: 07 set. 2023.

armazenados e utilizados, incluindo se serão compartilhados com terceiros; a importância da minimização de dados: somente os dados estritamente necessários para o objetivo pretendido devem ser coletados e processados; bem como o princípio da finalidade: os dados de saúde só podem ser usados para os fins para os quais foram coletados, a menos que se obtenha um novo consentimento para um uso diferente; a necessidade de ter a *accountability* e governança: instituições de saúde devem adotar práticas de governança de dados, incluindo políticas de privacidade claras, treinamento de funcionários e auditorias regulares; a comunicação de incidentes: caso ocorra uma violação de dados, há requisitos rigorosos sobre notificar as autoridades e, em alguns casos, os indivíduos afetados; a responsabilidades compartilhadas: quando diferentes entidades, como hospitais, laboratórios e seguradoras, estão envolvidas no tratamento de dados de saúde, é crucial definir claramente as responsabilidades de cada um, por fim, e, não menos importante, o encarregado de dados que é a nomeação de um encarregado de dados é obrigatório para supervisionar e garantir a conformidade com a LGPD.

Assim, verifica-se que a aderência à LGPD pode aumentar a confiança do paciente, que se sentirá mais seguro ao fornecer informações pessoais a médicos, sendo que falhas de proteção de dados podem expor médicos e ações legais por negligência ou violação de confidencialidade, que podem ser financeiramente e profissionalmente devastadoras.

3 DIRETRIZES PARA ADEQUAÇÃO DA LGPD EM CONSULTÓRIOS MÉDICOS

A LGPD é uma realidade que não pode ser ignorada por consultórios médicos. Além das implicações legais, estar em conformidade com a LGPD é uma forma de construir confiança com os pacientes. A adaptação à nova legislação é um processo contínuo que exige vigilância e atualização constantes. Em um mundo de mudanças, que correspondem a novas abordagens na coleta e uso de dados, é imprescindível propor soluções e discussões práticas relacionadas à privacidade.

O primeiro passo é identificar quais dados são coletados (que se dá através do data *mapping)* e o enquadramento em bases legais autorizadoras específicas, onde serão analisados a forma como os dados pessoais são armazenados e para

quais finalidades são usados, sendo que todos os dados pessoais que não tiverem finalidade objetiva deverão ser excluídos, pois estará desajustado com o Princípio de Necessidade e, ao invés de ser enquadrado em alguma base legal autorizadora específica, sugere-se que ele seja excluído.

Logo, o consentimento explícito para a coleta e o tratamento de dados é crucial. O paciente deve ser informado sobre como seus dados serão usados e ter a opção de consentir ou não. O consentimento é uma das bases legais mais comuns para o tratamento de dados pessoais, incluindo dados de saúde. No entanto, em algumas circunstâncias e de acordo com legislações específicas como a LGPD no Brasil, o tratamento de dados de saúde pode ser realizado sem o consentimento do titular, por exemplo, sob a base legal da "tutela da saúde", conforme artigo 11, f da referida lei. Quando o consentimento é utilizado como base legal, ele deve ser livre, informado e inequívoco. Isso significa que o titular dos dados deve ser plenamente informado sobre como seus dados serão usados, por quem e para quais finalidades, e deve concordar explicitamente com esse uso. Em situações onde o consentimento é exigido, é fundamental que este seja documentado de forma adequada. Geralmente, isso envolve manter registros do consentimento e garantir que o titular dos dados possa facilmente retirar seu consentimento a qualquer momento.

Por outro lado, segundo a Lei Geral de Proteção de Dados (LGPD), a "tutela da saúde" é uma das bases legais que autorizam o tratamento de dados pessoais relacionados à saúde sem a necessidade de obter o consentimento do titular[12]. De acordo com a LGPD, essa base legal se aplica exclusivamente em procedimentos realizados por profissionais da área da saúde, serviços de saúde ou autoridade sanitária. Isso significa que, em contextos específicos como diagnóstico médico, tratamento e outros serviços relacionados à saúde, o tratamento de dados pessoais sensíveis é permitido sem o consentimento do titular, desde que realizado por entidades ou profissionais devidamente qualificados na área da saúde. Vale ressaltar que mesmo se a base legal for a tutela da saúde, ainda são necessárias medidas rigorosas para proteger a privacidade e a segurança dos dados. Isso inclui limitar o

---

[12] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 set. 2023.

acesso aos dados apenas a profissionais autorizados e garantir que os dados sejam utilizados apenas para as finalidades específicas para as quais foram coletados. Assim, enquanto o consentimento do titular dos dados pode não ser necessário neste caso, a transparência e as medidas de segurança são fundamentais para cumprir as obrigações legais e éticas relacionadas à proteção de dados pessoais.

Adotar medidas de segurança, como criptografia e controle de acesso, é essencial para proteger os dados. A nomeação de um Encarregado de Dados, DPO (*Data Protection Officer*), pode ser designado para garantir a conformidade com a LGPD. Outro ponto crucial é o treinamento de funcionários, todos colaboradores devem ser treinados sobre os princípios da LGPD e em como lidar com dados pessoais de forma segura.

Em resumo, a Lei Geral de Proteção de Dados (LGPD) no Brasil impacta significativamente as clínicas médicas, pois elas lidam com informações sensíveis de pacientes, devendo seguir alguns passos importantes:

1. Consentimento: Obter o consentimento explícito dos pacientes para coletar e usar seus dados. 2. Segurança: Implementar medidas de segurança robustas para proteger os dados armazenados. 3. Transparência: Informar aos pacientes como seus dados serão utilizados e por quanto tempo serão armazenados. 4. Acesso e Correção: Permitir que os pacientes acessem seus próprios dados e corrijam informações incorretas. 5. DPO (*Data Protection Officer*): Designar um responsável pela proteção de dados. 6. Treinamento: Treinar funcionários e profissionais de saúde sobre a importância da proteção de dados e as obrigações legais.

A área da saúde é conhecida por muitos escândalos de problemas que já existiram – por exemplo, a "máfia das próteses".[13] Assim, essa área precisa se defender e mostrar que tem práticas de mercado adequadas para garantir benefício ao paciente e ao consumidor final, dependendo do produto. Foi a partir da "máfia das próteses" que os planos de saúde e seguradoras começaram a criar procedimentos para evitar fraudes, entre eles a prevenção de que os dados pessoais sejam compartilhados.

---

[13] BRASIL. Câmara dos Deputados. **CPI – Máfia das órteses e próteses no Brasil**. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-mafia-das-orteses-e-proteses-no-brasil. Acesso em: 13 set. 2022. n.p.

Existem vários casos de vazamento de dados na área da saúde que são noticiados globalmente[14], esses incidentes ilustram[15] os riscos associados ao manuseio inadequado de informações médicas sensíveis.[16] Cada um desses exemplos não só coloca os pacientes em risco mas também pode resultar em consequências legais sérias para as instituições de saúde envolvidas, incluindo multas e ações judiciais. Além disso, a reputação da instituição pode ser seriamente prejudicada, levando a perda de confiança por parte dos pacientes e, em alguns casos, a falência da instituição. É por isso que a conformidade com leis como a LGPD é tão crítica na área da saúde. Portanto, é crucial adotar práticas em conformidade com a lei.

CONCLUSÃO

Neste artigo, demonstramos que com a entrada em vigor da LGPD, as empresas devem introduzir em suas culturas diretrizes que visem a proteção dos dados pessoais e sensíveis, em resposta às necessidades de proteção efetiva das pessoas, na era em que vivemos de rápidas mudanças e avanços tecnológicos. Para que a lei tenha mais credibilidade e aderência, há imposição de multa pecuniária que pode chegar até 2% do faturamento da empresa, em casos de até R$ 50 milhões de faturamento. Em vista da alta pena pecuniária que poderá ser imposta e a perda de reputação, o assunto envolvendo a proteção de dados deve ser levado a sério.

Insta registrar que não é de hoje a ideia de proteção dos dados dos pacientes, não sendo exigência exclusiva da LGPD. Na Constituição Federal[17] já se tem a

---

[14] VAZAMENTOS de dados de saúde coloca consumidor em risco; veja o que fazer. *In:* INSTITUTO Brasileiro de Defesa do Consumidor. [*S. l.*], 2020. Disponível em: https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer. Acesso em: 05 set. 2023.

15 MÁFIA das próteses coloca vidas em risco com cirurgias desnecessárias. **G1**, São Paulo, 4 jan. 2015. Fantástico. Disponível em: https://g1.globo.com/fantastico/noticia/2015/01/mafia-das-proteses-coloca-vidas-em-risco-com-cirurgias-desnecessarias.html. Acesso em: 05 set. 2023.

16 NOVA falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. **G1**, São Paulo, 2 dez. 2020. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 05 set. 2023.

[17] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em:

obrigatoriedade de proteger a privacidade e a intimidade, além de prever o sigilo de correspondência e o *habeas data,* assim como outras leis também tratam de de proteção de dados, tais como o marco civil da internet, o Código de Defesa do Consumidor e o Código Civil.

Com o avanço tecnológico, os dados passaram a ser a porta lateral de acesso à intimidade e privacidade das pessoas, fenômeno que impactou diversos setores da sociedade. A multiplicação dos dados trouxe inúmeros benefícios para a área da saúde, mas também atraiu riscos; como por exemplo, o fornecimento de CPF nas farmácias possibilitou que os fornecedores possam ter mais elementos para incentivar o consumo de determinados produtos ou serviços. Dessa forma, vimos aumento da cobiça mercantil por dados de saúde, em decorrência da possiblidade de serem utilizados para atividades distintas da atividade assistencial.[18]

Diante dos riscos que todo esse impacto representa aos indivíduos, um dos objetivos da lei foi justamente dar diretrizes de implementação dentro de clínicas médicas. A adequação à Lei Geral de Proteção de Dados (LGPD) em clínicas médicas é de extrema importância por diversas razões, eis que o tratamento de dados de saúde permite o acesso da intimidade e da privacidade do indivíduo em graus que somente o titular (e mais ninguém) tem acesso.

A classificação, pela LGPD, como sensíveis, é o primeiro passo de uma efetiva política pública voltada a tutelar com maior intensidade os dados de saúde, cabendo aos controladores e operadores a proteção do paciente, pois o manuseio inadequado de dados médicos sensíveis pode ter sérias implicações para a privacidade e bem-estar do paciente. Reiterando, a não conformidade com a LGPD pode resultar em sanções severas, incluindo multas elevadas e danos à reputação da clínica, suspensão de atividades, proibição de operar dados, bem como, processos éticos, penais e indenizatórios. Assim, tem-se a necessidade de gestão de riscos, posto que a adequação à LGPD ajuda na implementação de melhores práticas para a gestão segura de dados, minimizando o risco de vazamentos ou mau uso de informações. Na verdade, o cumprimento da LGPD pode aumentar a confiança dos pacientes na

---

http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 24 jan. 2023.

[18] DANTAS, Eduardo; TRAD, Giovanna; DADALTO, Luciana; GUIDI, Silvio. **Comentários à Lei Geral de Proteção de Dados Sob a Perspectiva do Direito Médico e da Saúde.** Indaiatuba: Foco, 2023.

clínica, que saberão que suas informações estão sendo tratadas com o devido cuidado. Em um mercado cada vez mais digital e globalizado, a conformidade com regulamentos de proteção de dados pode ser um diferencial competitivo.

A LGPD requer que as organizações sejam transparentes sobre como coletam, usam e armazenam dados, o que pode melhorar o relacionamento com os pacientes. A lei ajuda a criar um padrão de como os dados devem ser tratados, tornando mais fácil para as clínicas implementarem sistemas de gerenciamento de dados, com sistemas mais seguros e eficientes, os profissionais de saúde podem ter acesso mais rápido e seguro aos dados dos pacientes, o que pode ser crucial para o diagnóstico e tratamento.

Em resumo, a adequação à LGPD em clínicas médicas não é apenas uma obrigação legal, mas também uma necessidade ética e estratégica que beneficia tanto os pacientes quanto as próprias instituições de saúde. Um paciente que não autorizou que suas informações fossem visualizadas por outros profissionais além do seu médico ou a outros que não estejam vinculados ao segredo profissional pode acionar a ANPD e o Judiciário para realizar processo contra a instituição de saúde.

Deste modo, manter em segurança os dados e os processos que são desenvolvidos dentro das clínicas médicas e hospitais é essencial, em conjunto com todas as formas e regulamentações de dados pessoais e sensíveis supracitadas e o dever de segredo profissional. Assim, a LGPD foi inserida como um marco importante por abranger e aumentar a proteção dessas informações no setor da saúde.

REFERÊNCIAS

ANPD aplica a primeira multa por descumprimento à LGPD. *In:* GOV.BR. Ministério da Justiça e Segurança Pública. Brasília, DF, 2023. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-a-primeira-multa-por-descumprimento-a-lgpd. Acesso em: 07 set. 2023.

BARROS JÚNIOR, Edmilson de Almeida. **Direito Médico**. Brasil: Haikai Editora, 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 24 jan. 2023.

BRASIL. Câmara dos Deputados. **CPI – Máfia das órteses e próteses no Brasil**. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-mafia-das-orteses-e-proteses-no-brasil. Acesso em: 13 set. 2022.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 04 set. 2023.

CONSUMERS INTERNATIONAL. **Consumers International**: Strategy. [*S. l.*]: Consumers International, 2018. Disponível em: https://www.consumersinternational.org/media/155232/strategy-eng.pdf. Acesso em: 7 jul. 2021.

DANTAS, Eduardo; TRAD, Giovanna; DADALTO, Luciana; GUIDI, Silvio. **Comentários à Lei Geral de Proteção de Dados Sob a Perspectiva do Direito Médico e da Saúde**. Indaiatuba: Foco, 2023.

MÁFIA das próteses coloca vidas em risco com cirurgias desnecessárias. **G1**, São Paulo, 4 jan. 2015. Fantástico. Disponível em: https://g1.globo.com/fantastico/noticia/2015/01/mafia-das-proteses-coloca-vidas-em-risco-com-cirurgias-desnecessarias.html. Acesso em: 05 set. 2023.

NOVA falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. **G1**, São Paulo, 2 dez. 2020. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml. Acesso em: 05 set. 2023.

SANTOS, Rafa. Regulamento avança na aplicação da LGPD ao disciplinar dosimetria das penas. **Consultor Jurídico**, São Paulo, 27 fev. 2023. Disponível em: https://www.conjur.com.br/2023-fev-27/regulamento-avanca-aplicacao-lgpd-disciplinar-penas. Acesso em: 07 set. 2023.

TERMOS de uso e política de privacidade. *In:* HOSPITAL Israelita Albert Einstein. São Paulo, 2022. Disponível em: https://www.einstein.br/sobre-einstein/politicas-site. Acesso em: 07 set. 2023.

VAZAMENTOS de dados de saúde coloca consumidor em risco; veja o que fazer. *In:* INSTITUTO Brasileiro de Defesa do Consumidor. [*S. l.*], 2020. Disponível em: https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer. Acesso em: 05 set. 2023.

WARREN, Samuel D.; BRANDEIS, Louis D. Right to Privacy. **Harvard Law Review**, Boston, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em:

https://www.cs.cornell.edu/~shmat/courses/ cs5436/warren-brandeis.pdf?. Acesso em: 16 jun. 2021.

12. RESPONSABILIDADE CIVIL E O TRATAMENTO DE DADOS PESSOAIS NAS CIRURGIAS ROBÓTICAS

https://doi.org/10.36592/9786554600712-12

Victória Maltchik Salles Jung[1]

RESUMO

Considerando que o tratamento dos dados pessoais não é vedado no ordenamento jurídico brasileiro, sendo a matéria regulada e, inclusive, apontada no rol dos direitos fundamentais, esta pesquisa visa investigar a relação entre a responsabilidade civil e o manejo dos dados pessoais dos pacientes submetidos à cirurgia robótica. O questionamento que se pretende resolver, então, é: quais são as exigências e as consequências legais do tratamento dos dados pessoais nos procedimentos cirúrgicos robóticos? Para isso, tem-se como objetivo verificar as normas e os princípios norteadores da Lei Geral de Proteção de Dados Pessoais a fim de compreender os efeitos do mau gerenciamento dos dados pessoais daqueles que estão envolvidos nos procedimentos médicos realizados por robôs dotados de inteligência artificial. Considerando que o número de participantes na realização de procedimento médico-hospitalar é extenso, tem-se como hipótese a dificuldade em se encontrar um único responsável quando da identificação do mau gerenciamento dos dados pessoais dos pacientes. Ademais, acredita-se que muitos inconvenientes podem ser evitados se apresentando o termo de consentimento esclarecido aos que são submetidos a tratamentos, diagnósticos e procedimentos com tecnologia diferenciada. Metodologicamente, a abordagem é dedutiva, uma vez que se parte de conceitos e princípios gerais do direito constitucional e civil para se alcançar resultados particulares em relação ao tratamento de dados pessoais no âmbito médico-hospitalar. Enquanto método de procedimento tem-se o estruturalista e, por fim, a interpretação sistemática através de uma técnica quali-quanti, a qual se utiliza de um referencial qualitativo para compreender a dimensão quantitativa dos dados abordados. A fim de viabilizar a pesquisa, buscar-se-á por fontes bibliográficas e documental. Espera-se com esse estudo, portanto, contribuir com o diálogo sobre a gestão ética dos dados pessoais na área da saúde.

Palavras-chaves: Direitos fundamentais; responsabilidade civil; dados pessoais; inteligência artificial.

ABSTRACT

Considering that the processing of personal data is not prohibited in the Brazilian legal system, and the matter is regulated and even pointed out in the list of

[1] Advogada licenciada. Mestranda em Direito na área de Fundamentos Constitucionais do Direito Público e do Direito Privado pela PUCRS. Bolsista CNPq. Membro do Grupo de Pesquisas Avançadas em Direito Tributário - GTAX. E-mail: victoria.maltchik@acad.pucrs.br.

fundamental rights, this research aims to investigate the relationship between civil liability and the management of personal data of patients undergoing robotic surgery. The question that is intended to be resolved, then, is: what are the requirements and legal consequences of the processing of personal data in robotic surgical procedures? To this end, the objective is to verify the norms and guiding principles of the General Law on the Protection of Personal Data to understand the effects of the mismanagement of the personal data of those involved in medical procedures performed by robots equipped with artificial intelligence. Considering that the number of participants in the performance of medical-hospital procedures is extensive, it is hypothesized that it will be difficult to find a single person responsible when identifying the mismanagement of patients' personal data. Moreover, it is believed that many inconveniences can be avoided by presenting the informed consent form to those who are submitted to treatments, diagnoses, and procedures with differentiated technology. Methodologically, the approach is deductive since it starts from general concepts and principles of constitutional and civil law to achieve results in relation to the processing of personal data in the medical-hospital environment. As a method of procedure, there is the structuralist and, finally, the systematic interpretation through a quali-quanti technique, which uses a qualitative reference to understand the quantitative dimension of the data addressed. To make the research feasible, bibliographic, and documentary sources will be sought. It is expected with this study, therefore, to contribute to the dialogue on the ethical management of personal data in the health area.
Keywords: Fundamental rights; civil liability; personal data; artificial intelligence.

INTRODUÇÃO

A tecnologia está presente na vida do ser humano desde os primórdios, mas alguns aspectos passaram a ganhar mais ênfase a partir da revolução industrial, ocorrida no século XVIII. Resumidamente, a máquina introduzida nas fábricas trouxe controvérsias no setor, consolidando o pensamento de que houve um processo evolutivo tecnológico, o qual trouxe mudanças sociais e econômicas[2]. Desde então, diversos estudos surgiram a fim de verificar os aspectos sociais, econômicos, jurídicos etc. deste fenômeno.

Para Theodor Adorno e Max Horkheimer, a razão humana leva a construção de máquinas que destroem, ou seja, ela perpassa uma lógica destrutiva, na qual quanto mais evolui, mais se destrói[3]. A revolução industrial potencializou a

[2] TOMASEVICIUS FILHO, E. **Inteligência artificial e direitos da personalidade:** uma contradição em termos? pp. 113-149. Revista da Faculdade de Direito, Universidade de São Paulo, 2018.
[3] ADORNO, T. W.; HORKHEIMER, M. **Dialética do esclarecimento:** fragmentos filosóficos. Rio de Janeiro: Zahar, 1985.

dimensão em que homem e a máquina protagonizaram articulações, as quais interferiram em múltiplas áreas da sociedade, demandando uma nova reflexão ética sobre a intersecção desses elementos no mundo contemporâneo. Desde então, a interação entre humano e não humano vislumbra avanços em meio às contradições[4].

Ao contrário, Jürgen Habermas se afasta da perspectiva marxista, defendendo que os avanços da racionalização, pelos quais a tecnologia é englobada, não acarreta necessariamente na "jaula de aço" proposta por Weber e repensadas por Adorno e Horkheimer[5]. Mais intensas são as críticas de Bruno Latour, que pensa ser interessante agregar o "novo", o "atual". Em suas obras, o autor discorre acerca da forte ligação entre humanidade, comunicação e tecnologia[6].

Semelhantemente, tem-se a atual discussão sobre o uso da inteligência artificial em diversos setores da sociedade. O presente estudo, porém, limita-se a analisar brevemente seu impacto dentro dos procedimentos cirúrgicos, mais especificamente quando da constatação de dano ao paciente em decorrência do vazamento de seus dados pessoais. A proposta aqui, então, não é avaliar a assertividade ou não da inserção da inteligência artificial na área médico-hospitalar, mas sim verificar quais são as consequências atribuídas ao seu uso.

Isso pois, não se pode retirar do mundo aquilo que a ele já foi inserido, cabendo ao homem estudar, discutir e desenvolver aquilo que já existe. Nesse sentido, Juarez Freitas e Thomas Bellini Freitas dizem: "os sistemas jurídicos, de modo praticamente uníssono, são convocados a enfrentar uma novíssima questão comum que quebra as barreiras, paradigmas e limites nacionais: a responsabilidade jurídica que advém da IA"[7 p,121].

---

[4] *Idem.*

[5] GENARO, E. **O debate da Teoria Crítica sobre tecnologia**, pp. 292-299. São Leopoldo: Ciências Sociais Unisinos, 2017.

[6] ARAÚJO, R. F. **Apropriações de Bruno Latour pela ciência da informação no Brasil:** descrição, explicação e interpretação. 2009. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal de Minas Gerais, Minas Gerais, 2009.

[7 p,121] FREITAS, J.; FREITAS, T. B. **Direito e Inteligência Artificial:** em defesa do humano. Belo Horizonte: Forum, 2020.

INTELIGÊNCIA ARTIFICIAL, DADOS PESSOAIS E ÉTICA: DEFINIÇÕES E RELAÇÕES

A inteligência artificial (IA) é um campo multidisciplinar da ciência da computação que aborda a construção de sistemas que possuem capacidade de realizar tarefas antes, normalmente, construídas por seres humanos. A IA consiste em técnicas e algoritmos de aprendizado de máquina, processamento de linguagem natural, raciocínio baseado em casos, otimização, redes neurais artificiais, lógica entre outros. Normalmente, o seu objetivo é desenvolver sistemas que possam analisar e interpretar dados, após a apreensão deles, possibilitando através disso, inclusive, tomada de decisões e resolução de problemas complexos de forma autônoma pela IA[8].

Já a definição de dados pessoais pode variar de acordo com a legislação estudada. Para fins didáticos, porém, tem-se que são quaisquer informações relacionadas a uma pessoa física identificadas ou identificáveis, direta ou indiretamente, como: nome, endereço, número de identificação, informações financeiras, localização, características físicas etc.[9]. Lembra-se que nem todos os dados são classificados como sensíveis, sendo exemplos deles: orientação sexual, etnia, saúde e religião[10]. Basicamente, a diferença entre dados pessoais e dados pessoais sensíveis é que os últimos incluem informações sobre a pessoa que são considerados especialmente confidenciais e privadas, podendo ser usadas de forma discriminatória.[11]

Relevante esclarecer que até o ano de 2022 os dados pessoas não era expressamente tido como um direito fundamental. O que se fazia até o momento era relacioná-lo ao direito fundamental à privacidade e ao *habeas data*, os quais são dispostos no artigo 5º, incisos X e XII, respectivamente, da Constituição Federal

[8] BORDINI, R. Inteligência Artificial. Apresentado em 28 de abr. 2021. Apresentador: Rafael Bordini. Apresentado no grupo de estudos interdisciplinar de Ciência da Coputação e Direito, realizado virtualmente em Porto Alegre, RS.
[9] BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados. Disponível em <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm > Acessado em 27/03/2023.
[10] SARLET, G. B. S.; RUARO, R. L. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018**. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021.
[11] *Idem.*

(CF/88), com intuito de que ele se valesse da qualidade de fundamental também[12]. Como leciona Ingo Sarlet, alguns dos direitos sociais e ecológicos não expressos capítulo de direitos fundamentais podem, mediante interpretação extensiva a outro direito já tido como fundamental, ser lido como tal, desde que seja demonstrada a sua vinculação.[13]

Nesse contexto, Ingo Sarlet e Giovani Saavedra apontam que:

> (...) o direito à proteção de dados pessoais pode (e mesmo deve!) ser associado e reconduzido a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental (também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam - aqui nos termos da CF - os direitos à privacidade e à intimidade, no sentido do que alguns também chamam de uma "intimidade informática.[14]

Entretanto, os pensadores criticam a interpretação implícita da proteção dos dados pessoais ser um direito fundamental, sob a justificativa de que a positivação formal “carrega consigo uma carga adicional, ou seja, agrega (ou, ao mesmo, assim o deveria) valor positivo substancial em relação ao atual estado da arte no Brasil”.[15,pp.44-4]

Hodiernamente, com o advento da Emenda Constitucional 115/2022, a proteção de dados pessoais foi elevada ao grau de direito fundamental, localizando-se no artigo 5º, inciso LXXIX da CF/88.[16] Isso significa que a proteção de dados passou a gozar de máxima proteção no ordenamento jurídico brasileiro; esse direito

---

[12] SARLET, G. B. S.; RUARO, R. L. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018**. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021.

[13] SARLET, I. W. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2021.

[14] SARLET, I. W.; SAAVEDRA, G. A. **Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais.** Revista Direito Público, 2020.

[15,pp.44-4] SARLET, I. W.; SAAVEDRA, G. A. **Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais.** Revista Direito Público, 2020.

[16] BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988. Disponível em https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 21 mai. 2023.

está hígido a qualquer alteração por conta de seu enquadramento como cláusula pétrea.[17]

Normalmente, toda a ação que está regulada é tida como legalizada, porém, nem sempre elas obedecem aos mandamentos éticos. Para que se possa prosseguir e falar das relações entre o uso de IA e o tratamento de dados na esfera médico-hospitalar, é necessário que se tenha a compreensão da própria definição de bioética, a qual Maria Helena Diniz ensina como sendo:

> A bioética seria, em sentido amplo, uma resposta da ética às novas situações oriundas da ciência no âmbito da saúde, ocupando-se não só dos problemas éticos, provocados pelas tecnociências biomédicas e alusivos ao início e fim da vida humana, às pesquisas em seres humanos, às formas de eutanásia, à distanásia, às técnicas de engenharia genética, às terapias gênicas, aos métodos de reprodução humana assistida, à eugenia, à eleição do sexo do futuro descendente a ser concebido, à clonagem de seres humanos, à maternidade substitutiva, à escolha do tempo para nascer ou morrer, à mudança de sexo em caso de transexualidade, à esterilização compulsória de deficientes físicos ou mentais, à utilização da tecnologia do DNA recombinante, às práticas laboratoriais de manipulação de agentes patogênicos etc., como também dos decorrentes da degradação do meio ambiente, da destruição do equilíbrio ecológico e do uso das armas químicas. Constituiria, portanto, uma vigorosa resposta aos riscos inerentes à prática tecnocientífica e biotecnocientífica, como os riscos biológicos, associados à biologia molecular e à engenharia genética, às práticas laboratoriais de manipulação genética e aos organismos geneticamente modificados, que podem ter originado o aparecimento de novas doenças virais ou o ressurgimento de antigas moléstias mais virulentas, e os riscos ecológicos, resultantes da queimada, da poluição, do corte de árvores, do uso da energia nuclear, da introdução de organismos geneticamente modificados no meio ambiente ou da redução da biodiversidade. Como o know-how tecnocientífico e biocientífico levanta questões quanto à segurança biológica e à transmutação dos valores morais, apenas a bioética poderia avaliar seus benefícios, desvantagens e perigos para o futuro da humanidade.[18,pp.10-1]

---

[17] *Idem.*
[18,pp.10-1] DINIZ, M. H. **O estado atual do biodireito.** 7. ed., São Paulo: Saraiva, 2010.

Em síntese, a evolução tecnológica, ainda que agregue valor ao ser humano, encontra óbices éticos para sua efetivação, sobretudo no que diz respeito à vida e ao tratamento da vida, abrangendo toda o seu significado, inclusive a proteção dos dados pessoais, dos pacientes. Hipoteticamente, quando uma pessoa precisa ser submetida a determinado procedimento médico em caráter de urgência, ela precisa consentir com o todas as clausulas do tratamento? Será que a falta de sua anuncia para ser operada por um robô dotado de IA pode ser relativizada em prol de sua vida nos casos celeridade exigida? Não sendo obedecido o devido procedimento de colhimento do consentimento do paciente, quem é responsabilizado no caso de vazamento de seus dados pessoais? Esses são alguns dos questionamentos que instigam esta pesquisa, estando algumas das respostas esboçadas na próxima seção.

A RESPONSABILIDADE CIVIL NAS CIRURGIAS ROBÓTICAS

Desde os anos 2000, a empresa estadunidense *Intuitive Surgical* desenvolve o robô Da Vinci, o qual já foi usado em mais de seis milhões de procedimentos cirúrgicos no mundo.[19] Especificamente no Brasil, país objeto de análise, 17 mil cirurgias realizadas por robôs já aconteceram, sendo o Hospital Israelita Albert Einstein o pioneiro.[20] Nessa oportunidade, explica-se que o sistema Da Vinci é formado basicamente por três componentes, sendo um deles o console ergonômico no qual o médico cirurgião fica situado, realizando os procedimentos através de um *joystick.*[21]

Entre as qualidades do uso dessa tecnologia está a flexibilidade dos punhos do robô, os quais eliminam os tremores da mão humana, bem como permite um giro

---

[19] DA VINCI SURGERY. About da Vinci Systems: surgical robotics for minimally invasie surgery. Disponível em: https://www.davincisurgery.com/da-vinci-systems/about-da-vinci-systems. Acesso em: 18 mai. 2023.

[20] HOSPITAL ISRAELITA ALBERT EINSTEIN. Brasil comemora 10 anos de cirurgia robótica. Disponível em https://www.einstein.br/sobre-einstein/imprensa/press-release/brasil-comemora-10-ano s-de-cirurgia-robotica#:~:text=Da%20primeira%20opera%C3%A7%C3%A3o%20aos% 20dias,foi%20adquirido%20em%20meados%202017. Acesso em: 18 mai. 2023.

[21] KFOURI NETO, M. **Responsabilidade Civil do Médico**, p. 413. São Paulo: Ed. Revista dos Tribunais Ltda., 2019.

de 360º, levando à precisão no corte e sutura feitos nos pacientes.[22] Como consequência nota-se a diminuição da perda de sangue durante o procedimento, além de redução de dor e desnecessidade de medicação por mais tempo, visto a célere recuperação dos pacientes.[23]

Por outro lado, não se pode ignorar a dimensão negativa do uso do robô nos procedimentos cirúrgicos. As telecirurgias funcionam mediante os comandos proferidos pelo médico cirurgião ao sistema, o qual depende de uma rede virtual de *internet*, fazendo com que exista um tempo de latência entre a ordem dada pelo médico e o movimento realizado pelo robô.[24] Não suficiente, os sistemas são vulneráveis a ataques cibernéticos, podendo ser hackeados de modo a alterar o curso do procedimento.[26] Não bastasse isso, os dados pessoais dos operados estão sujeitos a vazamento.

Finalmente, chega-se à questão a ser estudada: em caso de dano causado aos pacientes durante os procedimentos cirúrgicos realizados pelos robôs, mais especificamente em relação aos dados pessoais vazados, quem a responsabilidade civil vincula? Inicialmente, cumpre situar que a responsabilidade civil, de forma abrangente, tem como finalidade a vedação de ofensas, mas se constatada, surge a obrigação de reparação, como leciona Pontes de Miranda.[25] Válido frisar que, segundo José Joaquim Canotilho, pode acontecer de atos ilegais não projetarem responsabilidade, pois nem sempre se caracteriza dano no caso concreto, sendo ele elemento necessário para configuração da responsabilidade civil.[27]

A fim de melhor entender a matéria, rememorar-se-á, rapidamente, pontos relevantes da responsabilidade civil; como regra geral, o Código Civil de 2002 (CC/02) aderiu a responsabilidade civil subjetiva, que tem como premissa a comprovação do dano e a verificação do nexo causal e culpa para vincular o ofensor

---

[22] *Idem.*
[23] KFOURI NETO, M.; NOGAROLI, R. **Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia:** uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). Revista Científica da Academia Brasileira de Direito Civil, Rio de Janeiro, 2020.
[24] VIEIRA, E. V. Responsabilidade civil dos profissionais envolvidos nas cirurgias robóticas. 2021. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais - UFMG, Belo Horizonte, 2021.
[26] MIRANDA, P. **Tratado de direito privado:** direito das obrigações. São Paulo: RT, 1984.
[27] CANOTILHO, J. J. G. **O problema da responsabilidade do Estado por actos lícitos.** Coimbra: Almedina, 1974.

ao dever de reparar. Veja-se, nessa toada, a redação do artigo 186: "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito"[28]

Não obstante, Sergio Cavalieri Filho aponta que nem sempre é viável provar a culpa do agente na sociedade moderna e aduz que o desenvolvimento industrial, entre outras situações, gera novos contextos que não são amparados pelo conceito tradicional de culpa.[29] Em decorrência disso, surge a teoria do risco integral que releva a discussão da culpa ao determinar o dever de reparar, podendo determinado sujeito ser responsabilizado civilmente ainda que não tenha comprovado a sua culpa no caso debatido.[30] A responsabilidade civil objetiva é encontrada no artigo 927, parágrafo único, do CC/02. Veja-se:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, **independentemente de culpa**, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (grifou-se).[31]

Retornando à discussão, os profissionais da saúde assumem um compromisso de "meio" e não de "resultado", ou seja, a sua obrigação não é para com a cura do paciente e sim com a prestação com zelo e promoção de cuidado para com os indivíduos por eles tratados.[32] Se constatado eventual dano sofrido pelos pacientes, é exigida a comprovação de culpa (imprudência, negligência ou imperícia).[33] Desse modo, nota-se que se fala em responsabilidade civil subjetiva, diferente do que pode ocorrer em casos envolvendo cirurgias estéticas, em que a busca pelo embelezamento está diretamente relacionada com uma obrigação de

---

[28] BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 20 mai. 2023.
[29] CAVALIERI FILHO, S. **Programa de responsabilidade civil.** São Paulo: Atlas, 2007.
[30] ZOCKUN, C. Z. **Da responsabilidade civil do Estado na omissão da fiscalização ambiental**, pp. 70-88. *In:* FREITAS, J. Responsabilidade civil do Estado. São Paulo: Malheiros Editores, 2006.
[31] BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília. Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em 20 mai. 2023.
[32] GONÇALVES, C. R. **Responsabilidade Civil:** de acordo com o novo Código Civil (Lei n. 10.406, de 10-1-2022). São Paulo: Saraiva, 2005.
[33] *Idem.*

resultado.[34]

No Código de Defesa do Consumidor (CDC) a responsabilidade civil, segundo as definições do artigo 14, é objetiva, sendo, portanto, dispensável a comprovação de culpa para a aferição de reparação civil. Sabendo que os hospitais oferecem serviços próprios aos pacientes, como de hospedagem, refeição, tratamento e etc.,a responsabilidade deles acaba por se enquadrar na categoria de fornecedor de serviços e, em razão disso, submete-se às regras do artigo 14, caput, do CDC, isto é, respondem objetivamente por algum dano causado aos internados.[35]

Em contraste, assim como percebido no Código Civil, a regra para os profissionais liberais, ainda que prestem serviços de consumo, exige a demonstração de culpa. A justificativa para isso, consta no artigo 14, parágrafo 4º do CDC, observa-se: "a responsabilidade pessoal dos profissionais liberais será apurada mediante a verificação de culpa".[36]

Ocorre que, erros decorrentes de cirurgias envolvendo robôs dotados de inteligência artificial não trazem respostas simples quanto à vinculação dos responsáveis pelo dano. Quem tem a obrigação de reparar o paciente? Algumas são as possibilidades, haja vista a rede de sujeitos envolvidos na atividade. Num primeiro momento, pensa-se na atuação do médico durante o procedimento: teria ele agido em conformidade com o esperado, evitando os elementos de culpa (imprudência, negligência ou imperícia)? Analisado o nexo causal e chegado à conclusão de que o médico não trabalhou da forma esperada, adequada, ele é chamado a reparar o dano causado.

Haverá vezes, entretanto, que ele não será o responsável pelos prejuízos ou será culpado junto com outros. Se o dano causado ao paciente advier de falha na higienização do equipamento robótico pelos técnicos de enfermagem e enfermeiros, eles serão obrigados civilmente, se comprovada a culpa. Sendo a inconsistência no próprio robô, serão os fabricantes e fornecedores os

---

[34] SILVA, E. C. Defesa Jurídica do cirurgião plástico. Migalhas, 2019. Disponível em: https://www.migalhas.com.br/depeso/300122/defesa-juridica-do-cirurgiao-plastico. Acesso em 20 mai. 2023.

[35] BRASIL. Lei nº 8.078 de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 21 mai. 2023.

[36] *Idem.*

responsáveis. Para chegar a esses desfechos, basta uma simples consulta à legislação civil e consumerista já citadas.

Entretanto, dois são os pontos mais curiosos: (i) Seria viável atribuir responsabilidade civil ao próprio robô? Aqueles dotados de inteligência artificial são considerados sujeitos de direitos com direitos e obrigações, de modo que a provocação de dano por ele possa obrigá-lo a reparação? (ii) O consumidor paciente tem liberdade de escolha de seu tratamento junto com o médico? Se sim, como se caracteriza a responsabilidade civil quando ausente termo de consentimento esclarecido?

Quanto ao primeiro questionamento, Paulo Caliendo faz referência "aos escolásticos, que desde Santo Agostinho, diferenciavam os seres conforme a capacidade de sentir e racionalizar".[37, p. 133] O docente segue seu raciocínio dizendo que não só se deve verificar a possibilidade de exigir inteligência emocional aos robôs dotados de inteligência artificial, como também necessitam de uma inteligência social; ter emoções não é suficiente, devendo os agentes morais artificiais reconhecer as emoções, bem como controlá-las e expressá-las competentemente quando em relacionamento com outras pessoas.[38]

Parecido disserta Maria Manuel de Matos Parente Vasconcelos ao lembrar que o robô dotado de inteligência artificial "não passa de uma combinação algorítmica que é fornecida ao software, à máquina, nunca se tratando aqui de uma ação ética, ou espiritual, ou de cuidado com o outro"[39,p. 33], motivo pelo qual não é possível que seja alargada a personalidade jurídica a fim de abranger essa nova figura. Outra crítica advém dos pensamentos de Eduardo Tomasevicius Filho ao falar que:

> Existe um problema de matriz filosófica, igualmente objeto de estudo da medicina e da psicologia, que é o fato de a inteligência artificial não se tratar de uma inteligência holística. Até o momento, ainda se limita a uma inteligência

---

[37,p. 133] CALIENDO, P. **Ética e Inteligência Artificial:** da possibilidade filosófica de Agentes Morais Artificiais. Porto Alegre, RS: Editora Fi, 2021.
[38] *Idem.*
[39,p. 33] VASCONCELOS, M. M. M. **Inteligência Artificial:** Direito e Personalidade Jurídica. 2020. Dissertação (Mestrado em Ciências Jurídico Forenses) - Universidade de Coimbra, Coimbra, 2020.

> lógico-matemática. Como se sabe, o ser humano tem inteligências múltiplas e já está superada a ideia de que inteligência é somente racionalidade.[40,pp. 133]

Do mesmo modo, Fabio Siebeneichler de Andrade e Lucas Girardello Faccio frisam que auferir personalidade jurídica aos robôs inteligentes não resolve as questões impostas à responsabilidade civil, devendo, mesmo assim, ser alcançado determinada pessoa que será vinculada ao dever de reparo, veja-se:

> Em essência, abstraindo-se as questões axiológicas e no plano da teoria geral do Direito, no ponto central da responsabilidade civil, a questão do eventual pagamento da indenização às vítimas, em princípio não se extrai uma contribuição central que a outorga da personalidade jurídica própria aos robôs, de modo a torná-los pessoas de pleno direito, no mesmo plano, por exemplo, das pessoas jurídicas. Essa solução não evitaria a necessidade de se alcançar um responsável, potencial e concretamente apto, no plano patrimonial, a fim de reparar o prejuízo causado. Precisamente no terceiro plano de propostas sobre o tema exposto, debate-se, em face da potencial utilização em massa dos mecanismos e bens dotados de inteligência artificial, acerca dos possíveis instrumentos capazes de propiciar melhores condições de proteção na hipótese de danos.[41,p. 174]

Com isso, percebe-se que a primeira hipótese já é, majoritariamente, rejeitada pela doutrina nacional, isto é, em caso de complicações em cirurgias envolvendo o uso de inteligência artificial, dificilmente o próprio robô será responsabilizado. Todavia, o segundo questionamento permanece: como ficam os casos em que não há um termo de consentimento esclarecido pelo paciente quanto a escolha de seu tratamento, ou, no caso aqui debatido, quanto ao uso de robô para viabilização de uma cirurgia?

A discussão acerca da autonomia do homem não é recente. O filósofo alemão, Immanuel Kant defende que a vontade humana é um dos aspectos mais

---

[40,pp. 133] TOMASEVICIUS FILHO, E. **Inteligência artificial e direitos da personalidade**: uma contradição em termos? pp. 113-149. Revista da Faculdade de Direito, Universidade de São Paulo, 2018.
[41,p. 174] ANDRADE, F. S. FACCIO, L. G. **Notas sobre a responsabilidade civil pela utilização da inteligência artificial.** Revista da AJURIS: Porto Alegre, 2019.

relevantes do ser humano e, ao mesmo tempo em que o autor entende que o homem é capaz de decidir o que deve ou não fazer, ele também é responsável pelas suas ações.[42] Sob essa perspectiva, tem sido dada a chance aos pacientes determinarem qual tratamento dentre os que lhe forem apresentados desejam seguir. Isso porque, o consentimento informado tem respaldo no direito geral de personalidade.[43]

No artigo 6º da Declaração Universal sobre Bioética e Direitos Humanos, ocorrida em 2005 pela Organização das Nações Unidas para Educação, Ciência e Cultura (UNESCO), consta que "qualquer intervenção médica preventiva, diagnóstica e terapêutica só deve ser realizada com o consentimento prévio, livre e esclarecido do indivíduo envolvido (...)".[44] O dever de informação, no Brasil, encontra-se positivado no Código de Ética Médica, Resolução do CFM n. 1.931, de 17/09/2009, estando o profissional submetido ao compromisso de revelar todas as informações pertinentes aos pacientes.[45]

Com base nos estudos publicados por Miguel Kfouri Neto e Rafaella Nogaroli, é sabido que o médico incorre em responsabilidade civil nos casos em que seus pacientes sejam submetidos a procedimentos cirúrgicos com participação de robô dotado de IA sem que antes haja o consentimento livre e esclarecido deles.[46] O debate existente, porém, versa sobre quem deve obter o consentimento dos pacientes. A título de exemplo, os autores apontam que na Califórnia cabe apenas ao médico assistente esse dever, uma vez que ele é quem estabelece uma relação mais próxima e de confiança com o sujeito operado.[47] Por outro lado, professor português André Gonçalo Dias Pereira entende pela responsabilidade solidária do dever de informar.[48]

Necessário ressaltar, no entanto, que a assinatura de termo de

---

[42] KANT, I. **Metafísica dos costumes.** Vozes: Petropólis, 2013.
[43] RODRIGUES, J. V. **O Consentimento Informado para o Acto Médico:** Elementos para o Estudo da Manifestação de Vontade do Paciente, p.25. Coimbra: Coimbra Editora, 2001.
[44] UNESCO. Declaração Universal sobre Bioética e Direitos Humanos. Disponível em https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_univ_bioetica_dir_hum.pdf. Acesso em: 20 mai. 2023.
[45] KFOURI NETO, M.; NOGAROLI, R. **Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia:** uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). Revista Científica da Academia Brasileira de Direito Civil, Rio de Janeiro, 2020.
[46] *Idem.*
[47] *Idem.*
[48] *Idem.*

esclarecimento consentido não retira a responsabilidade do profissional da saúde em caso de danos oriundos de mau exercício laboral, mas o documento apenas afasta aqueles danos esperados e devidamente informados caso eles não advirem de culpa *lato sensu.*[49]

CONSIDERAÇÕES FINAIS

Conforme trabalhado neste *artigo*, muitas são as correntes doutrinárias envolvendo o uso e avanço das tecnologias nos mais variados ramos da vida privada. Desde os grandes eventos históricos, há quem defenda, como Adorno e Horkheimer que as máquinas corroboram para a destruição humana. Outros pensadores divergem encontrando nelas ferramentas essenciais para o desenvolvimento da sociedade. Ao que importa, independentemente do posicionamento adotado, tem-se que a humanidade não será mais a mesma depois da existência da inteligência artificial. Isso porque dificilmente se consegue retirar do mundo aquilo que já foi nele inserido. Com essas premissas em evidência, cabe aos pesquisadores e acadêmicos canalizarem os estudos em prol da melhor utilização da inteligência artificial, sobretudo nos casos envolvendo as cirurgias robóticas.

Ainda que faltem algumas respostas e regulamentações nesse setor, conta-se com critérios objetivos para análise da responsabilidade civil nos casos em que pacientes submetidos à cirurgia robótica tenham alguma complicação decorrente do procedimento. Nesse sentido, observou-se que, em geral, a responsabilidade médica é subjetiva, dependendo, portanto, da comprovação de culpa. Isso ocorre porque a obrigação profissional é de *meio*, isto é, os médicos precisam garantir um eficiente e comprometido tratamento aos seus pacientes do início ao fim de seu contato com ele. Não obstante, não se pode esperar que ele tenha êxito em todos os casos atendidos; noutros termos: é descaracterizada a obrigação de *fim*.

Especificamente quanto à inteligência artificial, conhece-se que a legislação

---

[49] OLIVEIRA, V.; PIMENTEL, D.; VIEIRA, M. **O uso do termo de consentimento livre e esclarecido na prática médica.** Revista Bioética, vol. 18, núm. 3, 2010, pp. 705-724 Conselho Federal de Medicina Brasília, Brasil. Disponível em: https://www.redalyc.org/articulo.oa?id=361533254015. Acesso em 24 mai. 2023.

consumerista impõe a responsabilidade objetiva, a qual prescinde da comprovação de culpa, a todas as figuras que estejam envolvidas na relação de consumo: fabricantes, fornecedores, distribuidores, consumidores e etc. Com isso, caso algum robô dotado de inteligência artificial tenha alguma avaria ou aja em desconformidade com o esperado pelos programadores durante os procedimentos cirúrgicos, existe a possibilidade da configuração de responsabilidade civil objetiva e solidária daqueles que estejam envolvidos na cadeia consumerista do objeto. Nessas situações, o agir da equipe médica também será avaliado.

Diferentemente, todavia, deverá ser averiguado se o erro houve relação com alguma culpa, *lato sensu*, por parte dos profissionais da saúde ou não, haja vista que a legislação civil e consumerista atribui a responsabilidade subjetiva a esses. Ultrapassada essas considerações, questionou-se em que medida o próprio robô inteligente pode ser responsabilizado por algum erro durante a cirurgia. Nessa oportunidade, entendeu-se que ainda não se é viável atribuir personalidade jurídica a ele, afastando, então, qualquer hipótese de responsabilização da máquina.

Ato contínuo, estudou-se a necessidade de se apresentar um termo de consentimento esclarecido nos tratamentos médicos, sob o fundamento da autonomia da vontade e dignidade da pessoa humana. Em que pese o documento não seja restrito às situações envolvendo procedimentos cirúrgicos com robôs providos de inteligência artificial, sua relevância é ainda maior nesse contexto, porque muitos dos dados pessoais dos pacientes ficam armazenados e podem ser vazados ou hackeados por terceiros, fragilizando, assim, os direitos protegidos pela LGPD e reconhecidos enquanto fundamentais.

REFERÊNCIAS

ADORNO, T. W.; HORKHEIMER, M. **Dialética do esclarecimento:** fragmentos filosóficos. Rio de Janeiro: Zahar, 1985.

ANDRADE, F. S. FACCIO, L. G. **Notas sobre a responsabilidade civil pela utilização da inteligência artificial.** Revista da AJURIS: Porto Alegre, 2019.

ARAÚJO, R. F. **Apropriações de Bruno Latour pela ciência da informação no Brasil:** descrição, explicação e interpretação. 2009. Dissertação (Mestrado em Ciência da

Informação) - Universidade Federal de Minas Gerais, Minas Gerais, 2009.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 21 mai. 2023.

BRASIL. **Lei nº 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 18 mai. 2023.

BRASIL. **Lei nº 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Brasília. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 18 mai. 2023.

CALIENDO, P. **Ética e Inteligência Artificial:** da possibilidade filosófica de Agentes Morais Artificiais. Porto Alegre, RS: Editora Fi, 2021.

CANOTILHO, J. J. G. **O problema da responsabilidade do Estado por actos lícitos.** Coimbra: Almedina, 1974.

CAVALIERI FILHO, S. **Programa de responsabilidade civil**. São Paulo: Atlas, 2007.

DA VINCI SURGERY. **About da Vinci Systems**: surgical robotics for minimally invasie surgery. Disponível em: https://www.davincisurgery.com/da-vinci-systems/about-da-vinci-systems . Acesso em 20 mai. 2023.

FREITAS, J.; FREITAS, T. B. **Direito e Inteligência Artificial:** em defesa do humano. Belo Horizonte: Forum, 2020.

GENARO, E. **O debate da Teoria Crítica sobre tecnologia**, pp. 292-299. São Leopoldo: Ciências Sociais Unisinos, 2017.

GONÇALVES, C. R. **Responsabilidade Civil:** de acordo com o novo Código Civil (Lei n. 10.406, de 10-1-2022). São Paulo: Saraiva, 2005.

HOSPITAL ISRAELITA ALBERT EINSTEIN. **Brasil comemora 10 anos de cirurgia robótica.** Disponível em: https://www.einstein.br/sobre-einstein/imprensa/press-release/brasil-comemora-10-ano s-de-cirurgia-robotica#:~:text=Da%20primeira%20opera%C3%A7%C3%A3o%20aos%20dias,foi%20adquirido%20em%20meados%202017. Acesso em: 21 mai. 2023.

KANT, I. **Metafísica dos costumes**. Vozes: Petropólis, 2013.

KFOURI NETO, M. **Responsabilidade Civil do Médico**, p. 413. São Paulo: Ed. Revista

dos Tribunais Ltda., 2019.

KFOURI NETO, M. **Responsabilidade Civil dos Hospitais**, p. 540. São Paulo: Ed. Thomson Reuters, 2019.

KFOURI NETO, M.; NOGAROLI, R. **Responsabilidade civil pelo inadimplemento do dever de informação na cirurgia robótica e telecirurgia:** uma abordagem de direito comparado (Estados Unidos, União Europeia e Brasil). Revista Científica da Academia Brasileira de Direito Civil, Rio de Janeiro, 2020.

MIRANDA, P. **Tratado de direito privado:** direito das obrigações. São Paulo: RT, 1984.

OLIVEIRA, V.; PIMENTEL, D.; VIEIRA, M. **O uso do termo de consentimento livre e esclarecido na prática médica.** Revista Bioética, vol. 18, núm. 3, 2010, pp. 705-724 Conselho Federal de Medicina Brasília, Brasil. Disponível em: https://www.redalyc.org/articulo.oa?id=361533254015. Acesso em: 21 mai. 2023.

RODRIGUES, J. V. **O Consentimento Informado para o Acto Médico:** Elementos para o Estudo da Manifestação de Vontade do Paciente, p.25. Coimbra: Coimbra Editora, 2001.

SARLET, G. B. S.; RUARO, R. L. **A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018**. Revista Direitos Fundamentais & Democracia, v. 26, n. 2, p. 81-106, 2021.

SARLET, I. W. **A eficácia dos direitos fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. Porto Alegre: Livraria do Advogado, 2021.

SARLET, I. W.; SAAVEDRA, G. A. **Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais**, pp. 33-57. RDP: Brasília, 2020.

SILVA, E. C. **Defesa Jurídica do cirurgião plástico**. Migalhas, 2019. Disponível em: https://www.migalhas.com.br/depeso/300122/defesa-juridica-do-cirurgiao-plastico. Acesso em: 20/06/2020.

TOMASEVICIUS FILHO, E. **Inteligência artificial e direitos da personalidade:** uma contradição em termos? pp. 113-149. Revista da Faculdade de Direito, Universidade de São Paulo, 2018.

UNESCO. **Declaração Universal sobre Bioética e Direitos Humanos**. Disponível em: https://bvsms.saude.gov.br/bvs/publicacoes/declaracao_univ_bioetica_dir_hum.pdf. Acesso em: 20 mai. 2023.

VASCONCELOS, M. M. M. **Inteligência Artificial:** Direito e Personalidade Jurídica. 2020. Dissertação (Mestrado em Ciências Jurídico Forenses) - Universidade de Coimbra, Coimbra, 2020.

VIEIRA, E. V. **Responsabilidade civil dos profissionais envolvidos nas cirurgias robóticas**. 2021. Dissertação (Mestrado em Direito) - Universidade Federal de Minas Gerais - UFMG, Belo Horizonte, 2021.

ZOCKUN, C. Z. **Da responsabilidade civil do Estado na omissão da fiscalização ambiental**, pp. 70-88. In: FREITAS, J. Responsabilidade civil do Estado. São Paulo: Malheiros Editores, 2006.

13. PROTEÇÃO DE DADOS PELAS SERVENTIAS EXTRAJUDICIAS: UMA ANÁLISE A PARTIR DA LEI GERAL DE PROTEÇÃO DE DADOS (Lei 13.709/2018) E DO PROVIMENTO 134/CNJ

https://doi.org/10.36592/9786554600712-13

William Arthur Leonhardt Born[1]

SUMÁRIO

1 Introdução; 2 Do Tratamento de Dados pelo Poder Público; 3 Do Tratamento de Dados pelas Serventias Extrajudiciais; 4 Conclusão; Referências.

RESUMO

O presente trabalho trata da proteção de dados pelas serventias extrajudiciais (registros públicos e tabelionatos), a partir de uma leitura conjunta dos dispositivos da Lei Geral de Proteção de Dados – LGPD, com o provimento n.º 134, do Conselho Nacional de Justiça, de 24 de agosto de 2022. O trabalho está dividido em duas partes: a primeira parte consiste no tratamento de dados pelo poder público e as suas especificidades, em especial, visto que dentro dessa matéria se encontra a regulação do tratamento de dados pelas serventias extrajudiciais. Na segunda parte, abordar-se-á especificamente a proteção de dados pelos cartórios, a partir da análise da natureza jurídica de tais serventias, dos princípios e regramentos específicos da atividade, das peculiaridades no tratamento de dados e da necessidade de readequação. O objetivo do presente texto é analisar as mudanças trazidas pela LGPD e pelo Provimento n.º 134/CNJ.
Palavras-chave: Proteção de dados; Lei Geral de Proteção de Dados; Poder Público; Serventias Extrajudiciais; Cartórios.

1 INTRODUÇÃO

O estudo do tratamento de dados pelo poder público e pelas serventias extrajudiciais é atual e extremamente importante, diante das disposições trazidas pela Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Cada vez mais se concretiza o fato de que os dados pessoais possuem alto valor e relevância na

---

[1] Mestrando em Direito pelo Programa de Pós-Graduação em Direito (PPGD) da PUCRS, bolsista CAPES/PROEX integral, especialista em Direito Notarial e Registral (PUC-Minas), especialista em Família e Sucessões (FMP), advogado.
E-mail: williamarthurleonhardt@gmail.com.

atualidade, em especial, considerando os avanços tecnológicos e da sociedade em rede. A LGPD buscou garantir o direito à privacidade dos indivíduos, especialmente no que concerne aos seus dados pessoais, visando assegurar proteção e segurança jurídica no Brasil. Isto porque, o correto tratamento e compreensão dos dados garante melhores e mais eficientes mecanismos de avaliação de cenários e tendências.

Dentre as novidades introduzidas pela lei, no Capítulo VI, vislumbramos a possibilidade das pessoas jurídicas de direito público tratarem e compartilharem dados pessoais com a administração pública e as serventias extrajudiciais. O setor público atua no tratamento desses dados sob a ótica de um ato administrativo, logo deve-se observar o interesse e a finalidade pública na utilização das informações pessoais dos indivíduos.

A Lei de Proteção de Dados visa garantir o equilíbrio entre essas forças, de forma a possibilitar que se alcance os melhores proveitos possíveis do tratamento de dados pessoais, especialmente pelo Poder Público sem que seja lesado o complexo jurídico da personalidade dos cidadãos brasileiros. Nesse sentido, as nomas garantem a proteção integral dos dados pessoais, a autodeterminação informativa e o respeito à privacidade dos titulares durante todo o ciclo do tratamento.

Desta forma, o trabalho foi dividido em dois pontos centrais: na primeira parte será analisado o tratamento de dados pelo poder público, e na segunda parte o tratamento de dados pelas serventias extrajudiciais diante das inovações trazidas pela LGPD e pelo Provimento n.º 134 do CNJ. Ao final realizar-se-ão as considerações finais.

Considerando as particularidades das serventias extrajudiciais que trabalham com dados pessoais diariamente, encontramos ampla quantidade de dados pessoais no serviço prestado desde a coleta, o armazenamento, o tratamento até o descarte desses dados, denotando-se uma fundamental análise pormenorizada dessa realidade. Desse modo, o presente trabalho busca responder as seguintes perguntas: Quais as mudanças trazidas pela LGPD e pelo Provimento n.º 134/CNJ nas serventias extrajudiciais? Há (in)compatibilidade entre a LGPD e a Lei de Registro de Registros Públicos em virtude do princípio da publicidade registral?

2 DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

A temática da proteção e dados pessoais tem sido evidenciada a partir do reconhecimento do direto à proteção de dados como direito fundamental integrando, portanto, o catálogo de direitos e garantias da Constituição Federal de 1988. O objetivo é proteger os direitos fundamentais da dignidade humana, do livre desenvolvimento da personalidade, do direito geral de liberdade, bem como direitos especiais de personalidade mais relevantes no contexto, quais sejam: os direitos à privacidade e à intimidade, o direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa[2].

A proteção dos dados pessoais tem como escopo garantir a proteção da privacidade dos indivíduos, com base no artigo 5º, inciso X da Constituição Federal. Essa privacidade pode ser compreendida pelo exercício do direito do seu titular em tornar público (ou não) as suas atividades aos entes sociais[3]. Isto porque, o espaço privado de cada sujeito e sua esfera de atuação é inviolável. Nesse contexto, os dados pessoais podem ser compreendidos como uma extensão da pessoa, por esse motivo são munidos de privacidade.

A Lei Geral de Proteção de Dados surgiu com o intuito de proteger os direitos fundamentais da pessoa natural ao estabelecer regras que forneçam um tratamento de dados pessoais em conformidade com os princípios e normas constitucionais e legais. No entanto, a LGPD não modificou as competências constitucionais dos entes nesse campo. Isto é, continua sendo de competência privativa da União legislar sobre essa matéria[4].

Diante desse cenário, a administração pública possui uma série de bancos de dados potencialmente sensíveis, sendo que a coleta e o tratamento desses dados é

---

[2] SARLET, Ingo W. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: MENDES, Laura S. DONEDA, Danilo. SARLET, Ingo W. RODRIGUES, Otavio Luiz Jr. BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

[3] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. Ed. Rio de Janeiro: Forense, 2020.

[4] BOTELHO, M. C.; CAMARGO, E. P. do A. O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA LGPD. **Revista Direitos Sociais e Políticas Públicas** (UNIFAFIBE), [S. l.], v. 9, n. 3, p. 558, 2022. DOI: 10.25245/rdspp.v9i3.1034. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/1034. Acesso em: 31 ago. 2023.

um ponto nevrálgico em termos de políticas públicas[5]. Por isso, salienta-se a necessidade de implementar de boas práticas no tratamento de dados pessoais, haja vista que podem auxiliar no atendimento aos comandos gerais da lei e prevenir a ocorrência de violações aos titulares[6].

Adentrando na temática do presente trabalho, destaca-se que as serventias extrajudiciais (tabelionatos e registros) são reguladas pelas normas concernentes aos dispositivos de tratamento de dados pelo poder público, ou seja, pelos dispositivos do Capítulo IV da Lei Geral de Proteção de Dados (Lei n. 13.709/2018). Dessa forma, devem seguir as mesmas regras do mesmo tratamento de dados dos componentes da Administração pública direta, como órgãos integrantes da administração direta dos poderes executivo, legislativo, incluindo as cortes de contas, e judiciário e do Ministério Público. Como também os componentes da administração pública indireta como as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela união, estados, distrito federal e municípios.

Em especial, ao que se refere aos cartórios, há a previsão do artigo 23, § 4º, que equipara os serviços notariais e de registros às pessoas jurídicas de direito público. Ademais, estabelece a obrigação dessas serventias de fornecer acesso aos dados por meio eletrônico para a administração pública, com o objetivo de atender a finalidade pública e de executar as competências legais ou cumprir as atribuições legais do serviço público (Art. 23, § 5, LGPD).

Sendo assim, o poder público e os cartórios devem respeitar os fundamentos, os princípios e as obrigações concernente ao tratamento de dados, exigindo a adoção das medidas previstas nessa lei. Esse tratamento deve atingir a finalidade púbica e na busca do interesse público. Por interesse público, entende-se a atuação estatal concretizada em conformidade com as forças de determinada sociedade, seja ela

---

[5] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). **LGPD**: Lei geral de proteção de dados comentada. 2 ed. São Paulo: Revista dos Tribunais, 2019. p. 246.

[6] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais.** Rio de Janeiro: Renovar. 2006. p. 409-410.

política, social, econômica, de forma a atender ao desenvolvimento de um maior número possível de pessoas[7].

Além do mais, deve-se observar os princípios que regem a administração pública, previstos no artigo 37 da Constituição Federal: legalidade, impessoalidade, moralidade, publicidade e eficiência. O tratamento de dados pessoais, de acordo com o artigo 23 da LGPD, tem como objetivo a execução das competências e a prestação dos serviços públicos nos termos da lei[8].

A regra geral, é de qualquer atividade envolvendo tratamento de dados depende do consentimento prévio e esclarecido do titular do dado pessoal[9]. No Guia Orientativo de 2022, a ANPD realça o aspecto intencional da manifestação, de forma que o titular dos dados deve ter total ciência dos fins de tratamento dos seus dados, com base no consentimento informado. Além disso, coaduna-se com o princípio da transparência da LGPD em que garante aos titulares o fornecimento de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento de dados, observados os segredos comercial e industrial (Art. 6º, VI, LGPD). Entretanto, a lei excepciona a necessidade desse consentimento nos casos: dos serviços públicos ou em decorrência do exercício de funções ou de competências previstas em norma legal, como é o caso dos cartórios.

Desse modo, o tratamento de dados pessoais pela Administração Pública não depende do consentimento do titular quando realizado para cumprir uma obrigação legal ou para realização de políticas públicas, desde que atenda à finalidade pública e ao interesse público[10]. No entanto, há que se especificar ao titular as hipóteses em que é feito o tratamento, juntamente com os procedimentos e as práticas usados. Esse tratamento é feito pelas pessoas jurídicas de direito público, no âmbito da sua competência legal e constitucional, mediante o fornecimento de informações claras

---

[7] PINHEIRO, Patrícia. P. **Proteção de Dados Pessoais**: comentários à lei nº 13.709/2018 – LGPD. São Paulo: Saraiva, 2018.

[8] TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do poder público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MALHOLLAND, Caitlin (org.). **A LGPD e o marco normativo no Brasil**. Porto Alegre: Arquipélago editorial, p. 249, 2020.

[9] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 140.

[10] SANTOS NETO, Arnaldo B.; ISHIKAWA Lauro; MACIEL, Moises. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, Santo Ângelo, v. 16, n. 40, p. 163-177, set./dez. 2021. p. 168.

quanto às situações em que o tratamento de dados é realizado. Isto porque, o poder público não pode violar a privacidade de indivíduos, salvo nas hipóteses legalmente admitidas[11].

Em que pese essa regra de publicidade e de transparência das informações constantes nas repartições públicas, isso não garante de imediato o amplo acesso a qualquer informação, tendo em vista outros bens jurídicos protegidos pela Constituição[12]. Esse é o caso das serventias extrajudiciais, principalmente pela circunstância de haver dados sensíveis, no seu acervo, cuja publicidade é restrita.

Os dados pessoais são informações que permitem identificar uma pessoa natural, de acordo com o entendimento do art. 5º, I, LGPD. O tratamento de dados abrange várias atividades que permitem transformar um dado pessoal - informação "bruta" - em conhecimento sobre a pessoa quanto seu comportamento, suas condutas, suas orientações pessoais, etc.[13] Com base nisso, é importante distinguir os dados pessoais e os dados pessoais sensíveis, haja vista que serão protegidos e tratados de maneiras diferentes.

Os dados sensíveis estão relacionados a origem étnica, saúde, vida sexual, convicção religiosa, opinião política, filiação a sindicato, dados genéticos vinculados a uma pessoa, com base no art. 5º, II, LGPD. Pelo caráter mais íntimo e pessoal dos dados sensíveis, em regra, esses dados sequer devem ser coletados ou armazenados. Na hipótese de sua coleta, deve-se atender a uma finalidade específica, nesse caso, exigindo-se um tratamento ainda mais cauteloso.

Além disso, com base no artigo 11 da LGPD, o tratamento de dados sensíveis será feito em algumas situações específicas, tais como: o cumprimento de obrigação legal; a proteção da vida ou da incolumidade física do titular ou de terceiros; a tutela da saúde; a garantia à fraude ou à segurança do titular, entre outros. Salienta-se que

[11] AMARAL, Fernando. **Introdução à ciência de dados.** Rio de Janeiro: Alta Books, 2016. p. 78.
[12] SALGADO, Eneidad Desiree. **Lei de acesso à informação (LAI):** comentários à Lei nº 12.527/2011 e ao Decreto nº 7.724/2012. São Paulo: Atlas, 2015. p. 97.
[13] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 140.

os dados pessoais sensíveis não perdem a sua natureza ou proteção legal pelo fato de integrarem bases de dados públicas[14].

Com base nessa premissa, a Autoridade Nacional entendeu por pontuar em seu guia orientativo as bases legais previstas na LGPD que seriam mais pertinentes para o tratamento pelo Poder Público, seriam elas: o Consentimento (ART. 7º, I e ART. 11, I); o Atendimento de interesse público/legítimo (ART. 7º, IX); o Cumprimento de obrigação legal ou regulatória (ART. 7º, II e ART. 11, II, a); a Execução de políticas públicas (Art. 7, III e ART. 11, II, b). Conforme prevê o inciso XII do Art. 5º de LGPD, será considerado como consentimento a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Sendo assim, o tratamento dos dados que são de acesso público, contam com a publicidade inerente, portanto não precisam do consentimento do titular. Sendo que esses dados podem ter o tratamento realizado para novas finalidades, desde que se observem os propósitos legítimos e específicos para o novo tratamento, preservando os direitos do titular e respeitando os fundamentos e os princípios da LGPD[15].

Esse tratamento deve ser realizado com propósitos legítimos, específicos e explícitos. Esses objetivos devem ser informados ao titular e é vedado o tratamento posterior de forma incompatível com essas finalidades[16]. Ademais, o tratamento deve ser limitado ao mínimo necessário para a adequada realização daquele ato registral/notarial, com base no princípio da proporcionalidade, ou seja, somente se coletará os dados pertinentes. Sendo assim, o legítimo interesse da administração pública não pode violar direitos e liberdades do titular, exigindo que esta política de tratamento de dados seja balanceada entre os interessados e os titulares dos dados[17].

---

[14] TASSO, Fernando Antônio. Do tratamento de dados pessoais pelo poder público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados: comentada. São Paulo: Revista dos Tribunais, 2019. p. 280.

[15] MURARI, Geogia A. C.; SCHIAVON, Isabela N.; BARRETOS, Ronaldo A. Dados pessoais: tratamento realizado pelo poder público à luz da Lei Geral de Proteção de Dados. **Revista Judiciária do Paraná**, Curitiba, n. 22, p. 252, nov. 2021. Disponível em: https://www.revistajudiciaria.com.br/portfolio-posts/revista-judiciaria-do-parana-edicao-22/. Acesso em: 30/08/2023.

[16] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 139.

[17] BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 45, p. 103-127, abr. 2021.. Acesso em: 06/06/2023.

Nesse contexto, para a realização do tratamento de dados, é preciso estabelecer e seguir medidas que garantam a transparência na coleta, tratamento, armazenamento e descarte de dados pessoais. Isto porque, os dados pessoais não podem ser acessíveis a quem não tem necessidade. No entanto, é importante frisar que dados públicos não possuem quaisquer restrições de acesso, logo, sua divulgação deve ser assegurada a qualquer interessado, se enquadra na categoria de compartilhamento amplo. Enquanto as demais categorias de compartilhamento (restrito e específico) estariam protegidos[18].

Caso os dados pessoais, que possuem acesso público, forem utilizados para outras finalidades, isto é, se houver alteração na motivação do uso das informações pessoais ou da sua finalidade. Se faz necessário o enquadramento do uso em nova base legal autorizada pela LGPD, com atenção ao consentimento e à autorização do titular[19].

Juntamente com o respeito à transparência, é preciso respeitar a boa-fé, visto que, a preocupação é garantir que o titular possa assegurar que seus dados estão sendo tratados de forma segura, verídica e cumprindo a sua finalidade[20]. Além disso, é garantido o livre e o gratuito acesso aos titulares dos dados sobre quais informações se encontram no banco de dados da serventia.

Outro ponto que merece destaque é o uso compartilhado de dados, cuja definição está no art. 5º, XVI, LGPD, que consiste na comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bandos de dados pessoais por órgãos e entidades públicas no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização prévia específica. Esse compartilhamento de

---

[18] SANTOS NETO, Arnaldo B.; ISHIKAWA Lauro; MACIEL, Moises. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, Santo Ângelo, v. 16, n. 40, p. 163-177, set./dez. 2021. p. 170.

[19] MURARI, Geogia A. C.; SCHIAVON, Isabela N.; BARRETOS, Ronaldo A. Dados pessoais: tratamento realizado pelo poder público à luz da Lei Geral de Proteção de Dados. **Revista Judiciária do Paraná**, Curitiba, n. 22, p. 253, nov. 2021. Disponível em: https://www.revistajudiciaria.com.br/portfolio-posts/revista-judiciaria-do-parana-edicao-22/. Acesso em: 30/08/2023.

[20] PINHEIRO, Patrícia. P. **Proteção de Dados Pessoais**: comentários à lei nº 13.709/2018 – LGPD. São Paulo: Saraiva, 2018.

dados pelo poder público deve ser realizado atendendo a finalidades específicas como na execução de políticas públicas[21].

Para que os sistemas e repartições da administração pública possam trabalhar em conjunto, é necessário que os sistemas computacionais estejam aptos a proceder o intercâmbio de informações de forma eficaz e eficiente[22]. Em outras palavras, há que existir interoperabilidade entre os sistemas, a fim de proporcionar o compartilhamento dos dados, com base nas limitações legais. Dessa maneira, no caso de haver bases distintas, que são interoperáveis, há prejuízo à eficiência na execução das competências do poder público[23].

Antes de adentrar especificamente no tratamento de dados pelas serventias extrajudiciais, debate-se sobre o compartilhamento de dados do poder público com entes privados. A regra é a vedação desse compartilhamento, no entanto, há exceções legais previstas no art. 25, §1º da LGPD que merecem atenção.

Há a possibilidade de compartilhar dados dos órgãos públicos com particulares, nos casos que envolvem (i) a execução descentralizada da atividade pública na qual se exige a transferência para atingir o fim específico e determinado; (ii) quando se tratar de dados que forem acessíveis publicamente; (iii) quando houver previsão legal ou a transferência for respaldada em contratos e convênios; (iv) na prevenção de fraudes e irregularidades para proteger e resguardar a segurança a integridade do titular. Evidenciando-se, portanto, a necessidade de uma finalidade pública específica para que haja o compartilhamento de dados pessoais com entes privados[24]. Destarte, a publicidade não se confunde com a divulgação indiscriminada de informações, nem mesmo sendo o caso de livre acesso ou consulta.

---

[21] TEPEDINO, Gustavo; TEFFÉ, Chiara Antônia Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

[22] MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). **LGPD**: Lei geral de proteção de dados comentada. 2 ed. São Paulo: Revista dos Tribunais, 2019. p. 269.

[23] AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016. p. 89.

[24] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019. p. 142.

3 DO TRATAMENTO DE DADOS PELAS SERVENTIAS EXTRAJUDICIAIS

A fim de compreender melhor a temática principal do presente texto, menciona-se que os serviços notariais e de registros são realizados em caráter privado, por delegação do poder público, segundo prevê o artigo 236 da Constituição Federal. Isto é, o notário ou o registrador é um profissional de direito, dotado de fé pública, a quem é delegado a atribuição de velar pela segurança, validade, eficácia e publicidade dos atos e negócios jurídicos[25].

Em outras palavras, trata-se de um particular que presta um serviço público, com base no poder que lhe foi conferido, a partir da aprovação em concurso público de provas e títulos. As serventias extrajudiciais possuem, portanto, uma natureza híbrida de caráter público e privada.

A morosidade dos procedimentos judiciais, a burocracia e o alto custo econômico e social são características dos procedimentos judiciais no cenário brasileiro. A fim de garantir que a tutela dos direitos seja mais célere, surge e se desenvolve o movimento da desjudicialização (Lei 11.441/2007). Esse movimento, contribui no desenvolvimento de meios alternativos para a solução de controvérsias advindas das relações sociais e econômicas diárias, para além da via judicial.

As serventias extrajudiciais (registros públicos e tabelionatos) representam os maiores expoentes nesse processo de desjudicialização, de maneira que, ao passar dos últimos anos, tiverem suas competências e atribuições aumentadas, como decorrência desse movimento. A sociedade brasileira tem optado pela via extrajudicial dada a sua menor onerosidade, maior celeridade e maior simplicidade no trâmite na obtenção das suas necessidades sociais.

Nesse contexto, essas serventias promovem o acesso à justiça, de maneira eficiente e econômica. A importância dos Registros Públicos e dos Tabelionatos no processo de desjudicialização é inegável, haja vista que garantem, aos cidadãos, maior concretização de seus direitos fundamentais, sem necessitar recorrer ao judiciário para tal. Sobretudo, dado o fato que os cartórios atribuem segurança jurídica aos negócios e aos atos jurídicos da população.

---

[25] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 59.

Outrossim, esse movimento tem se ampliado e concretizado, com os avanços tecnológicos atuais, uma vez que as distâncias físicas não são mais um empecilho no acesso aos cartórios, por exemplo a possibilidade trazida pelo Provimento 100 do CNJ de lavrar escritura públicas de maneira online pela plataforma do e-notariado, resultando na matrícula notarial eletrônica, a partir da utilização de certificados digitais e de assinaturas eletrônicas. O progresso digital tem impactado na qualidade e na celeridade dos cartórios, agilizando demandas, diminuindo a distância e os deslocamentos, garantindo ainda mais o acesso à justiça. Dessa maneira, contribuindo para a pacificação social ao oferecer uma solução segura e eficiente ao cidadão.

Diante da maior adesão da sociedade brasileira pela via extrajudicial, juntamente com a digitalização dos serviços notariais e de registro, os cartórios começaram a coletar e a armazenar cada vez mais dados da população. Diante desse cenário, fez-se necessário proteger todos esses dados constantes nessas serventias. Nesse cenário, a Lei Geral de Proteção de Dados veio como uma forma de complementar os cuidados já previstos em lei, abrangendo além da veiculação de certidões, o compartilhamento de dados com terceiros[26].

No contexto específico do tratamento de dados pelos cartórios, o Conselho Nacional de Justiça editou o Provimento 134, em 24 de agosto de 2022, no qual estabelece medidas a serem tomadas para o processamento de dados por essas serventias extrajudiciais, com o objetivo de adequá-las às disposições contidas na Lei Geral de Proteção de Dados (Lei 13.709/2018). Cabe destacar a competência do CNJ na função regulatória das atividades prestadas nas serventias notariais e de registro, com fulcro no art. 236, §1º, da CF. Ademais, as serventias extrajudiciais são obrigadas a cumprir essas normas técnicas estabelecidas pelo poder judiciário, com base nos artigos 37 e 38 da Lei 8.935/1994, razão pela qual, devem seguir as disposições desse provimento.

As serventias trabalham com dados pessoais em seu dia a dia, isto significa que tratam dados, a partir da coleta, da recepção, da classificação, da utilização, da reprodução, da transmissão, entre outras atividades elencadas no artigo 5º, inciso X,

---

[26] KÜMPEL, Vitor Frederico; FERRARI, Carla Modina. **Tratado notarial e registral**: Ofício de Registro Civil das Pessoas Naturais. Vol. II. São Paulo: YL Editora, 2022. p. 329.

da LGPD, razão pela qual precisam respeitar as disposições previstas por essa lei, bem como seguir as diretrizes, os regulamentos, as normas, as orientações e os procedimentos expedidos pela Autoridade Nacional de Proteção de Dados Pessoais. Ainda mais pelo fato de que o tratamento de todos os dados e informações registradas em cartório são de responsabilidade do titular que deve seguir o que é inerente à função de prestação de serviço de interesse público, executando competências e atribuições legais[27].

Os cartórios ao tratarem dados pessoais devem se atentar aos princípios da finalidade, adequação e necessidade, com base no artigo 2º, do Provimento n.º 134/CNJ. Isto significa que devem colher somente os dados necessários para a prática daquele determinado ato, ou seja, para atender à finalidade da prestação do serviço. A atuação extrajudicial se norteará pela persecução do interesse público, com objetivo de executar as competências e desempenhar as atribuições legais e normativas que lhe foram conferidas.

Ressalta-se que o escopo de proteção dos dados pessoais dado pela LGPD não só envolve dados pessoais eletrônicos, como também protege os dados contidos em acervo físico. O artigo 5º, inciso IV da LGPD estabelece que os bancos de dados correspondem a um conjunto estruturado de dados pessoais, estabelecido em um ou vários locais, em suporte eletrônico ou físico. Esse dispositivo possui especial relevância para as serventias extrajudiciais, uma vez os seus bancos de dados possuem esse caráter híbrido tanto de documentos digitais quanto físicos (livros e fichas em formato papel).

Discute-se bastante que a LGPD atingiria um dos princípios basilares do sistema dos registros públicos que é o da publicidade dos fatos ou das situações subjetivas. O artigo 17 da Lei 6.015/73 (Lei dos Registros Públicos) estabelece que qualquer pessoa pode requerer certidão de registro sem informar ao oficial ou ao funcionário o motivo ou interesse do pedido. Isso porque é assegurado a qualquer cidadão o direito a informações de cunho público que constam nos cartórios. Estas

---

[27] XIMENES, Rachel L. C. Os cartórios e a proteção de dados. **Jornal Jurídico**. Vol. 05, n. 01, 2022. p. 53. Disponível em: https://revistas.ponteditora.org/index.php/j2/article/view/623. Acesso em 05/06/2023.

informações, pelo princípio da publicidade em face do cumprimento da lei, independem do consentimento do titular dos dados[28].

A publicidade é o resultado do princípio democrático que sempre imperou nas serventias extrajudiciais, no sentido de os atos podem ser vistos e controlados pela sociedade em geral, a qualquer tempo, com a emissão de certidões[29]. O intuito é maior segurança jurídica, à medida em que nenhum ato se manterá em sigilo perante o fomento social, possibilitando o acesso pleno de terceiros, ainda que constem em tais atos dados vinculados e pessoais de seus contratantes, opositores e demais entes atuantes (NALILI, 2021).

A publicidade registral decorre da fé pública de seus atos, conferindo segurança jurídica, juntamente com o efeito da oponibilidade do registro perante terceiros (oponibilidade *erga omnes*). Essa publicidade pode ter como objeto pessoas (Registro das Pessoas Naturais e Tabelionato de Protesto) ou envolver bens (Registro de Imóveis). Essa publicidade, que representa a essência dos registros, é fundamental, pois representa a maneira pela qual o terceiro tem acesso às informações constantes nas serventias, ficando vinculado ao conteúdo registrado[30].

No entanto, há registros dos quais não se pode fornecer certidão a qualquer interessado, visto que contam com uma publicidade restrita, ou seja, que somente será fornecida em casos especiais. A exemplo dos casos envolvendo a personalidade e a intimidade da pessoa tais como a adoção, a troca de sexo, entre outros. É garantida a privacidade daquela informação, daquele dado, que pode ser entendida como a garantia da não violação do espaço do sujeito[31].

Além do fato de que é dever do notário e do registrador garantir o sigilo sobre os documentos e os assuntos de natureza reservada, ou seja, íntima e privada com

---

[28] PINHEIRO, Patrícia. P. **Proteção de Dados Pessoais**: comentários à lei nº 13.709/2018 – LGPD. São Paulo: Saraiva, 2018.
[29] COSTA, Ricardo A. CUNHA, Carlos R. TORRES, Dennis J. A. O Direito Fundamental à Proteção de Dados Pessoais no Âmbito das Serventias Notariais. **Revista Argumentum**. v. 23. n. 3. p. 1046, Set-Dez 2022. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1713. Acesso em 05/07/2023.
[30] KÜMPEL, Vitor Frederico; FERRARI, Carla Modina. **Tratado notarial e registral**: Ofício de Registro Civil das Pessoas Naturais. Vol. II. São Paulo: YL Editora, 2022. p. 328.
[31] BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. Ed. Rio de Janeiro: Forense, 2020.

fulcro no artigo 30, inciso VI da Lei 8.935. A vista disso, não haveria qualquer conflito entre a Lei de Registros Públicos e a Lei Geral de Proteção de Dados.

Desse modo, a publicidade registral e notarial deve ser contextualizada, relida, a partir da ótica da proteção de dados, a fim de garantir a privacidade e de prevenir práticas discriminatórias que possam atingir o indivíduo. Sendo assim, há claramente uma dicotomia entre cumprir a obrigatoriedade dos atos extrajudiciais, obedecido o princípio da publicidade, dentro da observância aos novos direitos pessoais que se materializam[32].

As certidões emitidas pelos cartórios devem conter todas as informações obrigatórias do ato, do fato ou da situação, estabelecidas na legislação específica, com base nas particularidades de cada tipo de serventia (registro ou tabelionato). Porém, a emissão de certidões deve se adequar a proporcional finalidade de comprovação do fato, do ato ou da relação jurídica (artigo 21 do Provimento 134/CNJ). Apurar-se-á a adequação, a necessidade e a proporcionalidade de particular conteúdo, em relação à finalidade da certidão, quando este não for explicitamente exigido ou quando for apenas autorizado pela legislação específica (art. 21, parágrafo único do Provimento 134/CNJ).

Portanto, cabe aos cartórios zelar pelo cuidado com os dados informados, quando da emissão de certidões, isto porque, há casos que, apesar da Lei de Registros Públicos conferir a ampla publicidade daquele ato/fato/situação, algumas informações devem ser protegidas, afetando sua publicidade. É preciso uma leitura conjunta entre as normas e os regramentos notariais e registrais com as disposições contidas na Lei Geral de Proteção de Dados, sobretudo com base nos fundamentos (artigo 2º, LGPD) do respeito à privacidade (inciso I), da inviolabilidade da intimidade, da honra e da imagem (inciso IV) e dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania pelas pessoas naturais (inciso VII) e nas disposições do Provimento nº 134 do CNJ.

Ainda no que se refere à publicidade dos atos notariais e de registro, há outro ponto que merece maior análise, o qual se refere ao compartilhamento de dados com

---

[32] COSTA, Ricardo A. CUNHA, Carlos R. TORRES, Dennis J. A. O Direito Fundamental à Proteção de Dados Pessoais no Âmbito das Serventias Notariais. **Revista Argumentum**. v. 23. n. 3. p. 1046, Set-Dez 2022. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1713. Acesso em 05/07/2023.

centrais e órgãos públicos. Muito se discutia que esse compartilhamento poderia ferir os preceitos da LGPD, até que o artigo 23 do Provimento 134 do CNJ resolveu essa questão ao considerar a compatibilidade do compartilhamento com o regramento legal. Desse modo, as centrais eletrônicas compartilhadas e os órgãos públicos podem receber informações das serventias extrajudiciais, desde que sejam observados os critérios da adequação, da necessidade e da persecução da finalidade dos dados a serem compartilhados.

No caso específico do compartilhamento de dados com os órgãos públicos, pressupõe-se lei ou ato normativo do órgão solicitante, ou convênio ou outro instrumento formal (art. 24, Provimento 134/CNJ). Ademais, somente se fornecerá informações específicas, necessárias e proporcionais ao atendimento das finalidades da política pública. A exemplo disso é a obrigatoriedade dos cartórios em fornecer informações ao Instituto Brasileiro de Geografia e Estatística – IBGE (artigo 49 da Lei 6.015/1973) e ao Instituto Nacional de Seguridade Social – INSS (artigo 68 da Lei 8.212/1991). Deve-se observar os protocolos de segurança da informação e evitar-se a transferência de bancos de dados, a não ser quando estritamente necessária para a persecução do interesse público.

Diante do exposto, as serventias extrajudiciais devem se adequar às disposições contidas na LGPD e no Provimento nº 134 do CNJ, por isso, demonstraremos algumas medidas necessárias a serem tomadas com base no artigo 6º do referido provimento. Os notários e registradores são considerados “controladores” dos bancos de dados das serventias. Logo, compete-lhes tomar as decisões referentes ao tratamento de dados pessoais, devendo assegurar que a finalidade e os meios tratamento dos dados pessoais são aqueles necessários para o cumprimento das tarefas inerentes às suas funções e às suas competências legais[33].

O provimento 134/CNJ trouxe uma classificação trinária de dados pessoais, dividindo-os em: dados restritos, sensíveis e sigilosos. Os dados restritos são aqueles previstos nos artigos 45 (certidão que conste a situação de filho legitimado por matrimônio subsequente) e 95 (certidão que conste a situação de adoção) da Lei

---

[33] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 139.

6.015/1973 e no artigo 6º e seus parágrafos da Lei 8.560/1992 (certidões que conste que o filho é fruto de uma relação extraconjugal). Conforme mencionado anteriormente, os dados sensíveis são aqueles elencados no artigo 5º, inciso II da Lei 13.709/2018 (LGPD). Isto é, aquele que se refere a origem racial ou étnica, convicção religiosa, filiação política, orientação sexual, entre outros. Importante salientar que as restrições relativas aos dados sensíveis elencados no referido dispositivo não se aplicam ao caso de pessoa falecida, tendo em vista o disposto no artigo 41 da LGPD. Por fim, os dados sigilosos são aqueles previstos no artigo 57, §7º da Lei 6.015/1973 (quando houver alteração de nome, em razão de coação ou ameaça pela colaboração com a apuração de crime).

É dever do controlador adotar as medidas técnicas e organizativas para o tratamento de dados adequado, tais como: a nomeação de encarregado pela proteção de dados; mapear as atividades de tratamento e realizar seu registro; adotar medidas de transparência aos usuários sobre o tratamento desses dados; definir e implementar uma política de segurança da informação e uma política interna de privacidade e proteção de dados; criar procedimentos internos eficazes, gratuitos e de fácil acesso para o atendimentos dos titulares; treinamento e a capacitação da equipe da serventia que está envolvida com esses dados, entre outras. Além disso, cabe ao cartório categorizar os dados já armazenados em dados pessoais e dados pessoais sensíveis, visto que o tratamento de cada tipo de dado será distinto.

O operador dos dados é pessoa física ou jurídica que trata os dados pessoais para o controlador. Age, portanto, em nome do controlador, de forma dependente. Pode ser um preposto da serventia ou sujeito externo à serventia, desde que devidamente formalizado por instrumento jurídico válido, devendo ter aptidão técnica para tratar dados. No entanto, goza de certa autonomia e independência.

A figura do operador é de extrema importância, haja vista que será o responsável receber reclamações, prestar esclarecimentos e adotar as medidas necessárias para o correto tratamento de dados. O operador será indicado pelo titular da serventia, ora controlador, que irá orientar os escreventes e auxiliares sobre a adoção das medidas cabíveis.

Outro agente de tratamento nas atividades notariais e de registro, é o encarregado cujas atribuições estão contidas no artigo 41, §2º da LGPD. É uma

pessoa natural, apontada pelo titular da serventia, que irá realizar a comunicação entre o controlador, os titulares dos dados pessoais e a autoridade nacional. Essa contratação será feita conforme a natureza e o porte do cartório, podendo ser dispensada a contratação desse encarregado. No entanto, para serventias maiores e que tratam com maior volume de dados é obrigatória a figura do encarregado.

O controlador e o operador devem manter registro de todas as operações que realizarem, atendendo o objetivo de garantir o tratamento e a proteção dos dados pessoais, juntamente com o compromisso de adoção de medidas para esse fim. Ambos podem responder por eventual dano causado pela inobservância legal. Além disso, o controlador e o operador podem responder por perdas e danos, caso não adotarem as medidas técnicas adequadas à proteção dos dados pessoais.

Medidas de segurança devem ser implementadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Impõe-se a adoção de medidas que visam salvaguardar e mitigar riscos às liberdades civis e aos direitos fundamentais do titular, tais como: a indicação de um encarregado pela gestão da segurança do banco de dados da serventia, a realização de um plano de ações para a adoção das mediadas necessárias na gestão dos seus arquivos, entre outras.

Outrossim, os cartórios devem seguir o Provimento 74 da Corregedoria Nacional de Justiça, de 31 de julho de 2018, no qual se dispôs padrões mínimos de tecnologia da informação para segurança, integridade e disponibilidade de dados nos serviços notariais e de registro no Brasil. Esse provimento buscou incentivar e divulgar a implementação de mecanismos de segurança da informação, a fim de garantir confidencialidade, disponibilidade, autenticidade e integridade dos atos praticados nessas serventias.

Para isso, os cartórios, em sua grande maioria, vêm-se obrigados a contratar empresas prestadoras de serviço para manter seguro o backup dos arquivos. Desse modo, precisa-se compartilhar com essas empresas privadas as informações públicas disponíveis nos arquivos, correspondendo, em grande maioria, de dados pessoais. Com as disposições trazidas pela Lei Geral de Proteção de Dados, os cartórios precisam criar uma política de gestão de dados, com o propósito de garantir

que essas empresas privadas protejam os dados que possuem acesso. Em outras palavras, é mister assegurar que essas empresas também cumpram com as disposições concernentes à proteção de dados.

A autoridade judiciária competente e/ou a ANPD pode exigir de cada cartório a prova da conformidade das medidas técnicas e organizativas adotadas à consecução da finalidade legal: a proteção dos dados pessoais[34]. Muito embora, exija-se a implementação de medidas de segurança, a LGPD e o Provimento 134/CNJ não estabelecem quais as medidas e quais os padrões de segurança a serem adotados, de modo que será estabelecida com base na realidade e nas condições de cada serventia.

Em caso de acesso não autorizado, caberá a serventia a elaboração de um relatório de impacto (artigos 32 e 38 da LGPD), juntamente com um plano de resposta a incidentes de segurança. Caberá ao titular do cartório, diante da situação ora apresentada, adotar todas as medidas para a apuração das causas, buscar reduzir novos riscos, bem como da informação dos impactos causados aos titulares dos dados.

Além disso, o titular responsável deve comunicar ao poder judiciário, em especial ao Juiz Corregedor Permanente da comarca do cartório e à Corregedoria Geral da Justiça do estado no prazo máximo de 24 horas, juntamente com a comunicação da ANPD (art. 48, LGPD). Esse relatório de impacto deve conter a descrição dos tipos de dados pessoais coletados e os mecanismos de segurança até então adotados pela aquela serventia.

Logo, exigir-se-á do notário e do registrador maior controle, e mais eficiente, de todo acervo gerado e armazenado no cartório[35]. Com base nisso, há que se adotar medidas de compliance, de boas práticas e de governança, que consiste na adoção de ações em conformidade com os preceitos da lei proteção dos dados pessoais. O

---

[34] LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021. p. 145.

[35] LAW, Thomas. **A Lei geral de proteção de dados**. Tese de doutorado. 2020. Disponível em: https://tede2.pucsp.br/bitstream/handle/23402/2/Thomas%20Law.pdf. Acesso em: 29/08/2023.

compliance consiste em mecanismos simples e eficazes para o devido cumprimento das normas jurídicas e éticas[36].

Para que assim, os cartórios reforcem o seu compromisso com a transparência e com a integridade no tratamento dos serviços prestados. Caberá para cada serventia analisar e adotar o melhor procedimento quanto a forma que deverá ocorrer a coleta, o tratamento, o armazenamento dos dados[37].

Os titulares das serventias extrajudiciais devem conscientizar seus colaboradores, funcionários, sobre todas as boas práticas de tratamento de dados com base nas disposições da LGPD e do Provimento 134/CNJ. Em especial, tratar da importância do respeito à privacidade e à proteção das informações contidas na serventia. Para isso, deve-se proporcionar aos colaboradores palestras e cursos de capacitação voltadas a proteção de dados nos cartórios.

CONCLUSÃO

O estudo do tratamento de dados pelas serventias extrajudiciais é de extrema importância, visto que os cartórios trabalham diariamente com muitos dados pessoais. Traçou-se, no primeiro tópico, o tratamento de dados pelo poder público e as suas principais características, princípios e regulações. Os cartórios serão regulados pelas disposições do Capítulo VI da LGPD que trata do tratamento de dados pelo poder público, razão pela qual a análise desse ponto se fez necessária. Constatou-se que os princípios da necessidade, da adequação e da privacidade são as bases para esse tratamento no âmbito da administração pública e das serventias extrajudiciais.

No segundo tópico, aprofundou-se na temática específica do tratamento de dados pelos cartórios, partindo das disposições da Lei Geral de Proteção de Dados e do Provimento 134 do Conselho Nacional de Justiça que regula essa matéria. Traçou-se a necessidade das serventias de respeitarem os princípios inerentes à

---

[36] LIMA, Hilda Glícia Cavalcanti Lima; STINGHEN, Verde João Rodrigo; TEIXEIRA, Tarcisio. Motivações para a adequação das serventias extrajudiciais à LGPD: mudança cultural e conscientização. In: TEIXEIRA, Tarcísio et al. (Orgs.). **LGPD e cartórios**: implementação e questões práticas. São Paulo: Editora Saraiva, 2021.

[37] Ibid.

atividade, como o da publicidade, dialogando com os princípios e regras da LGPD como o respeito à privacidade e à personalidade de cada indivíduo. Os cartórios no Brasil ainda estão em processo de adaptação na implementação de medidas que busquem tratar dados corretamente. Por isso, buscou-se traçar os principais aspectos desse assunto, com vistas a aprofundar essa temática específica.

Com base no exposto, é possível concluir que as mudanças trazidas pela Lei Geral de Proteção de Dados e pelo Provimento 134/CNJ trouxeram inúmeras mudanças na dinâmica das serventias extrajudiciais. Os cartórios em todo Brasil devem se adequar as novidades trazidas por esses instrumentos legais. Apesar de todas as novidades, a Lei Geral de Proteção de Dados (Lei 13.709/2018) e a Lei de Registros Públicos (Lei 6.015/1973) não se confrontam, pelo contrário, uma complementa a outra ao regular suas matérias específicas.

REFERÊNCIAS

AMARAL, Fernando. **Introdução à ciência de dados**. Rio de Janeiro: Alta Books, 2016.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais**: a função e os limites do consentimento. 2. Ed. Rio de Janeiro: Forense, 2020.

BOTELHO, M. C.; CAMARGO, E. P. do A. O TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO NA LGPD. **Revista Direitos Sociais e Políticas Públicas** (UNIFAFIBE), [S. l.], v. 9, n. 3, p. 549–580, 2022. DOI: 10.25245/rdspp.v9i3.1034. Disponível em: https://portal.unifafibe.com.br:443/revista/index.php/direitos-sociais-politicas-pub/article/view/1034. Acesso em: 31 ago. 2023.

BRASIL. **Guia orientativo**: Tratamento de dados pessoais pelo poder público. Brasília, DF: Autoridade Nacional de Proteção de Dados, [2022]. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 06 jun. 2023.

BRASIL. **Lei nº 6.015 de 1973**. Lei dos Registros Públicos. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l6015compilada.htm. Acesso em: 05/07/2023.

BRASIL. **Lei nº 8.395 de 1994**. Estatuto dos notários e registradores. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8935.htm. Acesso em: 05/07/2023.

BRASIL, **Lei nº 13.709 de 2018**. Lei Geral de Proteção de Dados. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04/07/2023.

BRASIL, Conselho Nacional de Justiça. **Provimento 134 de 2022**. Disponível em: https://atos.cnj.jus.br/atos/detalhar/4707. Acesso em: 05/07/2023.

BUCHAIN, Luiz Carlos. Proteção de dados: legítimo interesse e consentimento. **Revista da Faculdade de Direito da UFRGS**, Porto Alegre, n. 45, p. 103-127, abr. 2021. DOI: https://doi.org/10.22456/0104- 6594.107259. Acesso em: 06/06/2023.

COSTA, Ricardo A. CUNHA, Carlos R. TORRES, Dennis J. A. O Direito Fundamental à Proteção de Dados Pessoais no Âmbito das Serventias Notariais. **Revista Argumentum**. v. 23. n. 3. p. 1035-1050, Set-Dez 2022. Disponível em: http://ojs.unimar.br/index.php/revistaargumentum/article/view/1713. Acesso em 05/07/2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar. 2006.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani (coords.). **Comentários à lei geral de proteção de dados: Lei 13.709/2018**. São Paulo: Revista dos Tribunais, 2019.

KÜMPEL, Vitor Frederico; FERRARI, Carla Modina. **Tratado notarial e registral**: Ofício de Registro Civil das Pessoas Naturais. Vol. II. São Paulo: YL Editora, 2022.

LAW, Thomas. **A Lei geral de proteção de dados**. Tese de doutorado. 2020. Disponível em: https://tede2.pucsp.br/bitstream/handle/23402/2/Thomas%20Law.pdf. Acesso em: 29/08/2023.

LIMA, Hilda Glícia Cavalcanti Lima; STINGHEN, Verde João Rodrigo; TEIXEIRA, Tarcisio. Motivações para a adequação das serventias extrajudiciais à LGPD: mudança cultural e conscientização. In: TEIXEIRA, Tarcísio et al. (Orgs.). **LGPD e cartórios**: implementação e questões práticas. São Paulo: Editora Saraiva, 2021.

LOUREIRO, Luiz G. **Registro Públicos**: teoria e prática. 11 ed. rev. amp., Salvador: Editora Juspodivm, 2021.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coords.). **LGPD**: Lei geral de proteção de dados comentada. 2 ed. São Paulo: Revista dos Tribunais, 2019.

MURARI, Geogia A. C.; SCHIAVON, Isabela N.; BARRETOS, Ronaldo A. Dados pessoais: tratamento realizado pelo poder público à luz da Lei Geral de Proteção de Dados. **Revista Judiciária do Paraná**, Curitiba, n. 22, p., nov. 2021. Disponível em:

https://www.revistajudiciaria.com.br/portfolio-posts/revista-judiciaria-do-parana-edicao-22/. Acesso em: 30/08/2023.

NALINI, José Renato. **Os princípios do direito registral brasileiro e seus efeitos**. Direito Imobiliário Brasileiro: Coord. Alexandre Guerra e Marcelo Benacchio, São Paulo, 2011.

PINHEIRO, Patrícia. P. **Proteção de Dados Pessoais**: comentários à lei nº 13.709/2018 – LGPD. São Paulo: Saraiva, 2018.

SALGADO, Eneidad Desiree. **Lei de acesso à informação (LAI):** comentários à Lei nº 12.527/2011 e ao Decreto nº 7.724/2012. São Paulo: Atlas, 2015.

SANTOS NETO, Arnaldo B.; ISHIKAWA Lauro; MACIEL, Moises. O tratamento de dados pessoais pelo poder público e o papel dos tribunais de contas. **Revista Direitos Culturais**, Santo Ângelo, v. 16, n. 40, p. 163-177, set./dez. 2021.

SARLET, Ingo W. **A eficácia dos Direitos Fundamentais:** uma teoria geral dos direitos fundamentais na perspectiva constitucional. 13 ed. Porto Alegre: Livraria do Advogado, 2018.

______________. Fundamentos Constitucionais: O Direito Fundamental à Proteção de Dados. In: MENDES, Laura S. DONEDA, Danilo. SARLET, Ingo W. RODRIGUES, Otavio Luiz Jr. BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

TASSO, Fernando Antônio. Do tratamento de dados pessoais pelo poder público. In: MALDONADO, Viviane Nóbrega; BLUM, Renato Opice (coord.). **LGPD**: Lei Geral de Proteção de Dados: comentada. São Paulo: Revista dos Tribunais, 2019.

TEPEDINO, Gustavo; TEFFÉ, Chiara Antônia Spadaccini. Consentimento e proteção de dados pessoais na LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (orgs.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

TERRA, Aline de Miranda Valverde; CASTRO, Diana Paiva de. A responsabilidade do poder público no tratamento de dados pessoais: análise dos artigos 31 e 32 da LGPD. In: MALHOLLAND, Caitlin (org.). **A LGPD e o marco normativo no Brasil**. Porto Alegre: Arquipélago editorial, p. 237-264, 2020.

XIMENES, Rachel L. C. Os cartórios e a proteção de dados. **Jornal Jurídico**. Vol. 05, n. 01, 2022. Disponível em: https://revistas.ponteditora.org/index.php/j2/article/view/623. Acesso em 05/06/2023.